RayTalk®
wireless professionals
www.raytalk.com

RA-696

Hot Spot Wi-Fi Access Point

MiMo Hot Spot AP Single Radio 2,4GHz up to 300Mbps (2Tx2R) & Multi Wireless Network Access Control, AAA Authentication, Authorization, Accounting

2.4GHz
2T2R
Industrial Grade
300Mbps HIGH SPEED MIMO
Single Radio
802.3af PoE
802.11 b/g/n
GbE 1000 Mbps
QoS
IP50

USER MANUAL

Declaration of Conformity

We, the under signed
RayTalk Industries Srl
Via Nicolino di Galasso 19
47899 Serravalle
Republic of SAN MARINO
Tel: +378 0549 901170
Fax: +378 0549 900890
Contact: Mr. Gianluigi Savioli
E-Mail: gianluigi.savioli@raytalk.com

declare under our own responsibility that the product :

Brand Name	RayTalk
Model	RA-696
Descriptions	Hot Spot Wi-Fi Access Point
Applicant	RayTalk Industries Srl

to which this declaration refers conforms with the relevant standards:

Standard	**Test**
EN 300 328 V1.7.1	Art. 3.2 (Radio)
EN 60950-1 2006+A11:2009	Art. 3.1a (LVD)
EN 301 489-17 V2.1.1	Art. 3.1b (EMC)
EN 301 489-1 V1.8.1	Art. 3.1b (EMC)
EN 50385 : 2002	Art. 3.1a (LVD)

We hereby declare that the essential radio tests suites have been carried out and that the above named product is in conformity with all the essential requirements of R&TTE Directive 1999/5/EC.

The technical construction file as required by the Conformity Assessment procedure is kept at the address of applicant.

The product RayTalk RA-696 has been tested and found to comply with the stated standards which are required by the article 6.4 of the R&TTE Directive of 99/5/EEC.

Note: the use of the present equipment in the Italian regulation is ruled by the following directives:

- ***D.Lgs 1.8.2003, n.259 articles 104 and 105 for private use***
- ***D.M. 28.5.2003 and further modifications for R-LAN and telecommunication services with public access***

Gianluigi Savioli / Amministratore Unico
RayTalk Industries Srl
Date: October 05th, 2012

Copyright Statement

© 2008-2012 RayTalk Industries ® Republic of San Marino.
All rights reserved. This user's manual is owned and copyrighted by RayTalk Industries, except what described and explicitly referred to third parties. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of RayTalk Industries.
Except as stated herein, none of the material may be copied, reproduced, distributed, republished, displayed, posted or transmitted in any form or by any means including, but not limited to, electronic, mechanical, photocopying, or otherwise, without the prior written consent of RayTalk Industries.
Permission is granted to display, copy, distribute the materials for personal, non-commercial use only, provided you don't modify or alter the materials and you retain any and all copyright and other proprietary notices contained in it.
Any unauthorized use may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes.

Disclaimer

RayTalk Industries reserves the right to change specifications without prior notice.
While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. RayTalk Industries shall be liable only to the degree specified in the terms of sale and delivery.

Permission to use this document is granted by RayTalk Industries subject to the following conditions.
All documents and related graphics are provided "as is" without warranty of any kind and are subject to change without notice. The entire risk arising out of their use remains with the recipient. In no event shall RayTalk Industries be liable for any direct, consequential, incidental, special, punitive or damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information).
Nothing on this document shall be construed as conferring any license under any of RayTalk Industries' or any third party's intellectual property rights.

Trademarks

The RayTalk Industries Srl ® trademark and design and other marks referenced herein are either trademarks or registered trademarks of RayTalk Industries Srl ®. Other products and company names mentioned herein may be the trademarks of their respective owners. RayTalk Industries Srl ® prohibits the use of any RayTalk Industries Srl ® trademarks without prior written Approval by RayTalk Industries Srl ®.
All other registered and unregistered trademarks in this document are the sole property of their respective owners.

RoHS Compliant

Restriction of Hazardous Substances Directive 2002/95/CE

RayTalk confirms that the RayTalk products RA-696 is in conformity with the directive 2002/95/CE dated 2003/01/27, usually called RoHS directive, concerning the limitation of dangerous substances for electric and electronics appliances since July 1, 2006.
In particular the products conform to clause 4 which forbids the use of the following elements:

– Lead
– Mercury
– Cadmium
– Hexavalant chromium
– Polybrominated biphenyls
– Polybrominated diphenylethers

All the answers and certificates from RayTalk partners and suppliers demonstrate that the materials and components used on the production process do not contain any of those prohibited substances or only limited to the specific cases that are allowed by the directive.
In consequence, RayTalk confirms that products RA-696 is in accordance with the RoHS directive.

This symbol (crossed out bin wheelie symbol according to WEEE Annex IV) indicates separate collection of waste electrical and electronic equipment in the EU countries.
Please do not throw the equipment into the domestic refuse. Please use the return and collection systems available in your country for the disposal of this product.

For more information please contact info@raytalk.com

Table of Contents

1 Before You Start 6
1.1 Preface 6
1.2 Document Conventions 6
1.3 Package Checklist 6
2 System Overview and Getting Started 7
2.1 Introduction of the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 7
2.2 System Concept 7
2.3 The MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 Hardware Overview 8
2.4 System Requirement 11
2.5 Installation Steps 11
2.6 Access Web Management Interface 10
3 Incorporate MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696to the Network 11
3.1 Network Requirement 11
3.2 Configure WAN Port 11
3.2.1 Static IP 11
3.2.2 Dynamic 11
3.2.3 PPPoE 12
3.2.4 PPTP 13
3.3 Internet Connection Detection 13
3.4 WAN Bandwidth Control 14
3.5 What is Zone 14
3.5.1 Port Role Assignment 15
3.5.2 Planning Your Internet Network 15
3.5.3 Configure Zone Network 15
4 Let Your Network Be a Wireless Network 17
4.1 System Wireless General Settings 17
4.2 Zone Wireless Settings 18
4.3 Zone Wireless Security 21
4.4 Wireless Layer 2 firewall 30
4.4.1 Generic Firewall Rules 30
4.4.2 Predefined and Custom Service Protocols 34
4.4.3 Advanced 35
5 Who Can Access the Network 36
5.1 Type of Users 36
5.1.1 Local 37
5.1.2 RADIUS 40

5.1.3 On-Demand User 44
5.1.4 Free Authentication 53
5.2 User Login 54
5.2.1 Default Authentication 54
5.2.2 Login with Postfix 54
5.2.3 An Example of User Login 54
6 Restrain the Users 55
6.1 Black List 55
6.2 Group 56
6.3 Policy 56
6.3.1 Schedule 58
6.3.2 Firewall 59
6.3.3 QoS Profile 62
6.3.4 Routing 63
6.3.5 User Privilege 70
7 Access Network without Authentication 71
7.1 DMZ 71
7.2 Virtual Server 72
7.3 Privilege List 73
7.3.1 Privilege IP 74
7.3.2 Privilege MAC 75
7.3.3 Privilege IPv6 75
7.4 Disable Authentication in Public Zone 76
8 User Login and Logout 77
8.1 Before Login 77
8.1.1 Login with SSL 77
8.1.2 Internal Domain Name with Certificate 78
8.1.3 Walled Garden 81
8.1.4 Walled Garden AD 82
8.2 After Login 83
8.2.1 Portal URL after successful login 83
8.2.2 Idle Timer 84
8.2.3 Multiple Login 85
9 Networking Features of a Gateway 86
9.1 IP Plug and Play 86
9.2 Dynamic Domain Name Service (DDNS) 87
9.3 Port and IP Forwarding 88

10 System Management and Utilities 89
10.1 System Time 89
10.2 Management IP Address List 90
10.3 IP Address for Accessing User Log 90
10.4 SNMP 91
10.5 Administration 92
10.6 Change Admin Passwords 95
10.7 Backup / Restore and Reset to the Factory Default 96
10.8 Firmware Upgrade 97
10.9 Restart 98
10.10 Network Utility 99
10.10.1 Wake-on-LAN 99
10.10.2 Ping 99
10.10.3 Trace Route 99
10.10.4 Show ARP Table 99
10.11 Monitor IP Link 100
10.12 Console Interface 101
11 System Status and Reports 104
11.1 Viewing the Status 104
11.1.1 System Status 104
11.1.2 Interface Status 106
11.1.3 Routing Table 107
11.1.4 Current Users 108
11.1.5 Session List 109
11.1.6 User Log 109
11.1.7 Local User Monthly Network Usage Report 112
11.1.8 System Related Logs 113
11.1.9 DHCP Lease 114
11.2 Notification 120
11.2.1 E-Mail 121
11.2.2 SYSLOG 122
11.2.3 FTP 123
12 Advanced Applications 125
12.1 Upload/Download Local User Accounts 125
12.2 RADIUS Advanced Settings 127
12.3 Roaming Out 128
12.4 Customizable Pages 130

Appendix A. Policy Priority 131
Global Policy, Authentication Policy and User Policy 131
Appendix B. WDS Management 132
Appendix C. RADIUS Accounting 133
1. Description 133
2. VSA configuration in RADIUS server (IAS Server) 133
3. VSA configuration in RADIUS server (FreeRADIUS) 136
Appendix D. On-demand Account types & Billing Plan 138
Appendix E. External Payment Gateways 152
1. Payments via Authorize.Net 152
2. Payments via PayPal 156
3. Payments via SecurePay 158
4. Payments via World Pay 159
Appendix F. Portal Page Customization 162
How External Pages Operate 163
Appendix G. Terminal Server Setup 166
Overview of Network Ticket Generator 166
Including RT-TO696RF into Your Network 168
Managing RT-TO696RF on the Web Management Interface 169
Setting Up RT-TO696RF with the POS Printer 170
Setting up RT-TO696RF with the RayTalk Hot Spot Wi-Fi Access Point or Internet Subscriber Gateway 170
Terminal Auto Setup (TAS – Only available on RT-TO696RF) 171

1 Before You Start

1.1 Preface

This manual is for WLAN service providers or network administrators to set up a network environment using the Hot Spot Access Point Wi-Fi RayTalk RA-696. It contains step-by-step procedures and graphic examples to guide MIS staff or individuals with slight network system knowledge to complete the installation.

1.2 Document Conventions

Caution:	Represents essential steps, actions, or messages that should not be ignored.
Note:	Contains related information that corresponds to a topic.
	Indicates that clicking this button will apply all of your settings.
	Indicates that clicking this button will clear what you have set before the settings are applied.
	Indicates that clicking this button will save the changes you made, but you must reboot the system upon the completion of all configuration settings for the changes to take effect.
*	The red asterisk indicates that information in this field is compulsory.

1.3 Package Checklist

The standard package of Hotspot Gateway Series RAYTALK RA-696 includes:

- MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696
- CD-ROM (with User's Manual and QIG)
- Ethernet Cable x 1
- Console Cable x 1
- Power Adapter (DC 5V) x 1
- Detachable antenna x 2

Caution:

It is highly recommended to use all the supplies in the package instead of substituting any components with other suppliers to guarantee best performance.

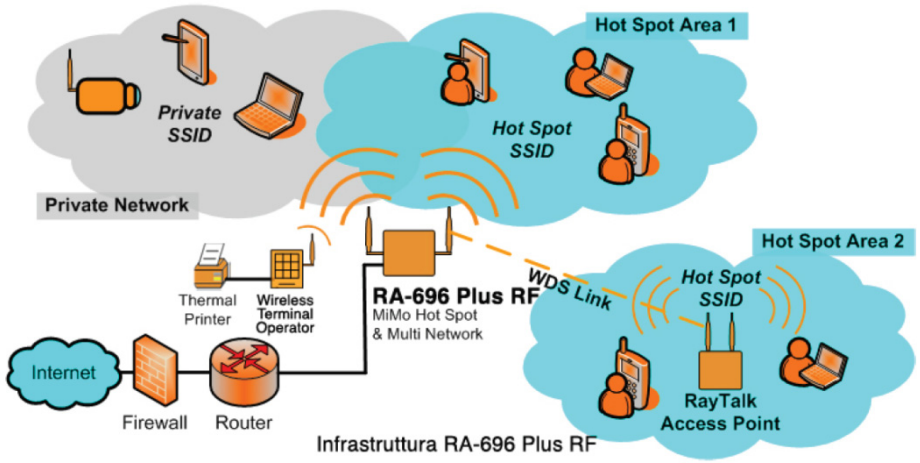
2 System Overview and Getting Started

2.1 Introduction of the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696

The **Hot Spot Access Point Wi-Fi RayTalk RA-696** is a feature-rich **Wireless Hotspot Gateway**, targeting realities that want to provide single-point wireless Internet access service. The RayTalk RA-696 is a perfect choice for beginners to run hotspot businesses. It does not cost much compared to buying a pile of equipment, nor does it take the skills of an expert to glue multiple applications out of multiple freeware. Feature-packed for hotspot operation, the RayTalk RA-696 comes with **built-in 802.11 n/b/g MIMO access point, web server and web pages for clients to login, easy logo-loading for branding a hotspot store, simple user/visitor account management tool, payment plans, multiple credit card gateways, traffic logs, IP sharing** and etc. The MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 also brings in an extra advantage - the wall-mountable IP50 dust-proof housing.

2.2 System Concept

The MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 is capable of managing user authentication, authorization and accounting. The user account information is stored in the local database or a specified external RADIUS database server. Featured with user authentication and integrated with external payment gateway, the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 allows users to easily pay the fee and enjoy the Internet service using credit cards through a variety of payment gateways including Authorize.Net, PayPal, SecurePay, and WorldPay. Furthermore, the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 introduces the concept of Service Zones – Private Zone and Public Zone, each with its own definable access control profiles. Private Zone means clients are not required to be authenticated before using the network service. However, clients in Public Zone are required to get authentication before using the network service. This is very useful for hotspot owners seeking to deploy wireless network service for clients and manage the network as well. The following diagram is an example of a MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 set to manage the Internet and network access services at a hotspot venue.



Example: A typical Hot Spot network

2.3 The MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 Hardware Overview

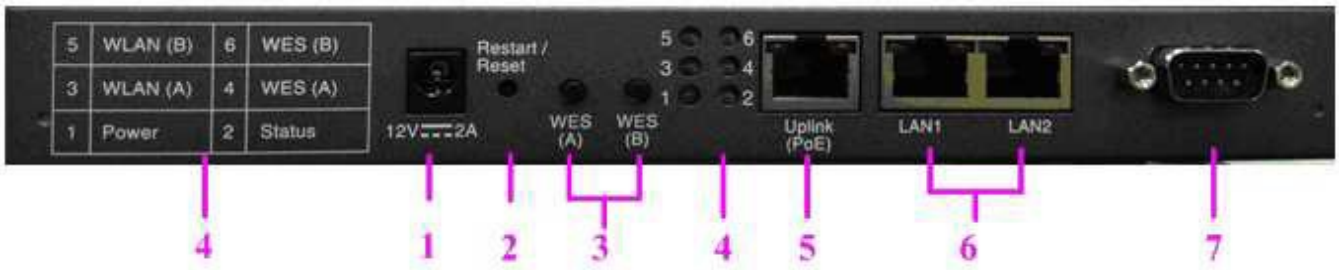
Rear Panel

1	**Antenna connector**	Reverse SMA connectors for attaching antenna as shown in above figure.
2	**WAN**	For attaching an Ethernet cable to an uplink service.
3	**LAN 1- 4 ports**	Attach Ethernet cables here for connecting to the wired local network.
4	**USB 2.0 port**	Reserved for future use.
5	**Console port**	Attach the serial cable here to access console interface.
6	**5V ⎓ 2 A**	Attach the power adapter here.
7	**Reset button**	Press once to restart the system; Press and hold for more than 5 seconds to reset to factory default.

Front Panel

1		**Quick button**	Press this button to quick-print an account generated from billing plan 1.
2		**WES button**	Press and hold over 5 seconds to initiate Master Mode for the WES process. Press and release to initiate Slave Mode for the WES process.
3		**Power LED**	On indicates power on.
4		**Status LED**	On indicates the system ready.
5		**Wireless LED**	On indicates wireless network interface is ready for service.
6		**WAN LED**	On indicates that WAN uplink connected.
7		**LAN1 - 4 LED**	Indicates the connection status of each LAN.
8		**USB LED**	Indicates the status of USB connection. USB port reserved for future use.
9		**WES LED**	For indicating WDS connection status.

	Master	Slave
WES Start	LED (Green) OFF and then BLINKING SLOWLY	LED (Red) OFF and then BLINKING SLOWLY
WES Negotiate	BLINKING NORMALLY (Green)	BLINKING NORMALLY (Red)
WES Timeout	LED (Green) ON	LED (Red) ON
WES Fail	LED (Green) ON	LED (Red) ON
WES Success	LED (Red) ON	LED (Green) ON



Rear Panel

1	**12V ⎓ 2A**	Power Jack Socket for the power adaptor.
2	**Restart / Reset**	Press once to restart the system; Press and hold for more than 5 seconds to reset to factory default.
3	**WES Button (A / B)**	WDS Easy Setup. Press the button to build up a WDS link with another peer. 4 WDS links can be set up per RF card.
4	**LED Indicators**	6 indicators that displays the states of 6 various functions or progresses. The numbers are explained on the leftmost side of the rear panel.
5	**WAN**	For attaching an Ethernet cable to an uplink service.
6	**LAN Ports 1 - 2**	The ports for connections with LAN side devices.
7	**Console Port**	To access RayTalk RA-696 via the console interface.

2.4 System Requirement

- Gigabit Ethernet network cables with RJ-45 connectors.
- All PCs need to install the TCP/IP network protocol.

2.5 Installation Steps

Please follow the steps mentioned below to install the hardware of the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696:

1. **Place the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 at the best location.**

The best location is usually at the center of your wireless network.

2. **To supply power to the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696.**

Connect the **power adapter** to the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696's power jack socket on the rear panel.

3. **Connect MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 to your outbound network device.**

Connect one end of the **Ethernet cable** to the WAN port of RAYTALK RA-696 on the rear panel. Depending on the type of internet service provided by your ISP, connect the other end of the cable to the ATU-Router of an ADSL, a cable modem, a switch or a hub. The WAN LED indicator should be ON to indicate a proper connection.

4. **Connect the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 to your PC.**

Connect one end of the **Ethernet cable** to the LAN1 port of the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 on the rear panel. Connect the other end of the cable to a PC for configuring the system. The LAN1 LED indicator should be ON to indicate a proper connection.

Note:

The MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 has two virtual **Private** and **Public zones** that are mapped to LAN1, LAN2 (192.168.10.254) and LAN3, LAN4 (192.168.11.254) respectively.

Now, the hardware installation is completed.

Caution:
Please use ***only*** *the power adapter supplied with the RAYTALK RA-696 package. Using a different power adapter may cause damage to this system.*

Caution:
To verify the wired connection between the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 and your switch/router/hub. Please check the LED status indication of these network devices.

2.6 Access Web Management Interface

The MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 supports Web Management Interface (WMI) configuration. Upon the completion of hardware installation, the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 can be configured via web browsers with JavaScript enabled such as Internet Explorer version 6.0 and above or Firefox.

Default LAN interface IP address:

Private Zone with IP 192.168.10.254, no authentication is required for users.

Public Zone with IP 192.168.11.254, by default authentication is required for users.

Note: The instructions below are illustrated with the administrator PC connected to LAN1.

To access the web management interface, connect a PC to **LAN1 Port**, and then launch a browser.

Make sure you have set DHCP in TCP/IP of your PC to "Obtain an IP address automatically". The default gateway IP address is the default gateway IP address of Private Zone: "192.168.10.254".

Next, enter the gateway IP address of the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 at the address field. The default gateway IP address of **LAN1 Port** is ***"https://192.168.11.254"*** (**"https"** is used for a secured connection).

The administrator login page will appear. Enter ***"admin"***, the default username, and ***"admin"***, the default password, in the **User Name** and **Password** fields.

Click ***LOGIN*** to log in.

After a successful login, a "Home" page with four main buttons will appear on the screen.

Caution:

If you can't get to the login screen, the reasons may be: (1) The PC is set incorrectly so that the PC can't obtain the IP address automatically from the LAN port; (2) The IP address and the default gateway are not under the same network segment.

Please set your PC with a static IP address such as 192.168.10.xx in your network and then try it again.

3 Incorporate MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696to the Network

3.1 Network Requirement

In the general network environment, the main role of the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 is to manage all the network access from internal network to Internet. Thus, the first step is to prepare an Internet connection from your ISP (Internet Service Provider) and connect it to the WAN port of the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696.

3.2 Configure WAN Port

There are 3 connection types for the WAN Port: **Static**, **Dynamic** and **PPPoE**. These connection types are enough to support most ISPs.

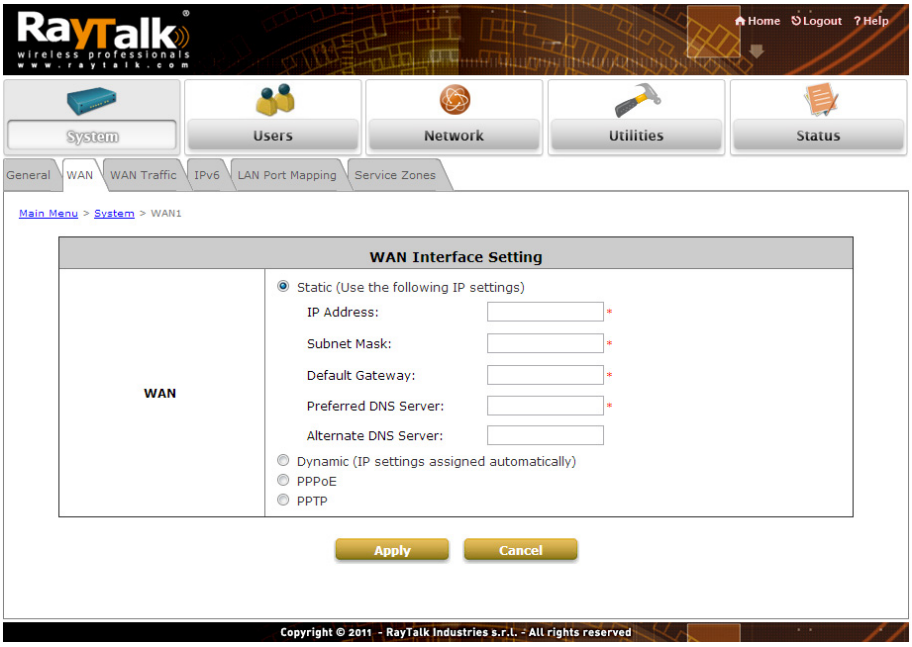
Now, let us discuss how to configure the WAN port. Go to: ***System >> WAN***.

The parameters related to each connection method are described in the following pages.

3.2.1 Static IP

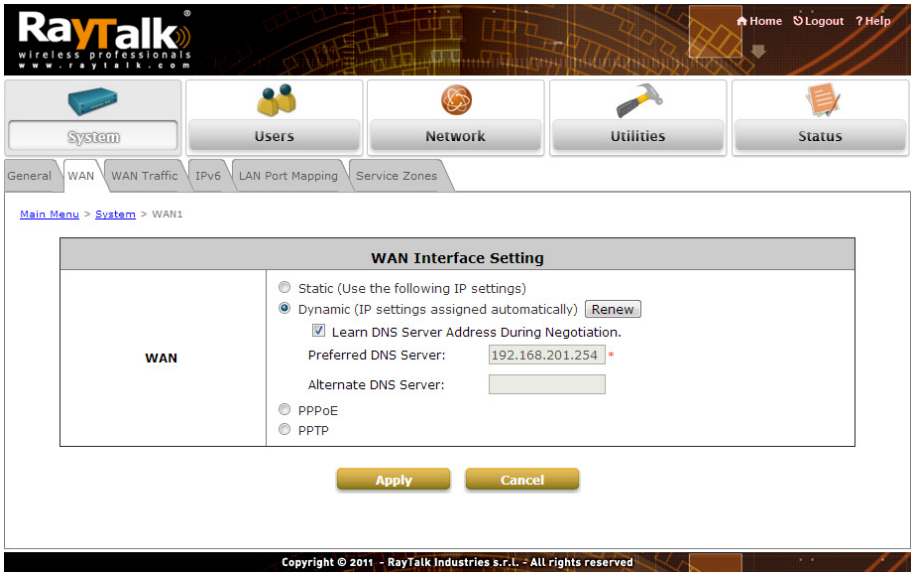
Static: Manually specifying the IP address of the WAN Port. The fields with red asterisks are mandatory.

- **IP Address:** The IP address of the WAN port.
- **Subnet Mask:** The subnet mask of the WAN port.
- **Default Gateway:** The gateway of the WAN port.
- **Preferred DNS Server:** The primary DNS Server of the system.
- **Alternate DNS Server:** The substitute DNS Server of the system. This is an optional field.



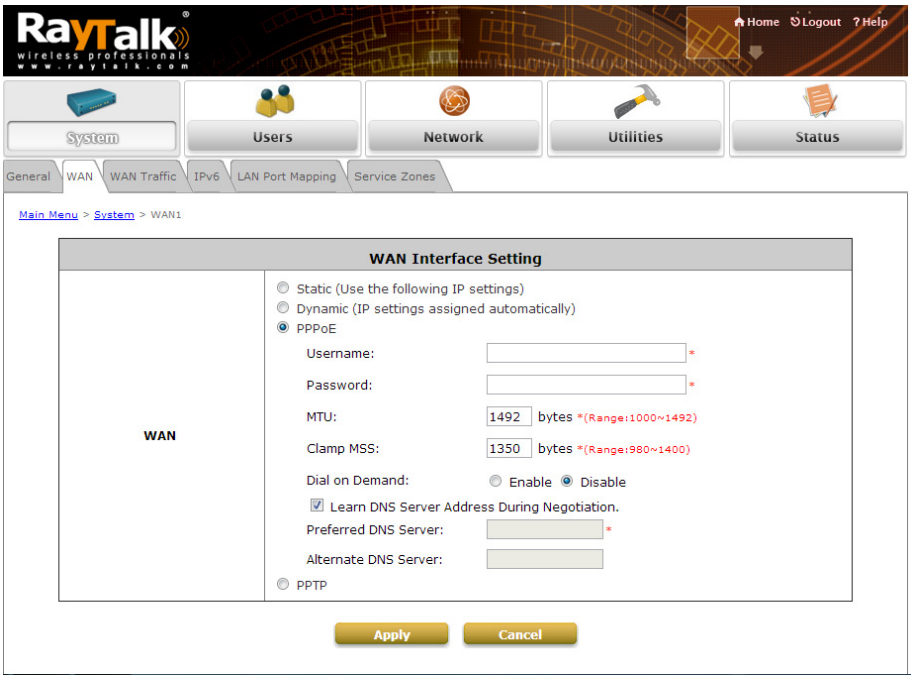
3.2.2 Dynamic

Dynamic: It is only applicable for the network environment where the DHCP server is available upstream of the system. Click the ***Renew*** button to get an IP address automatically.



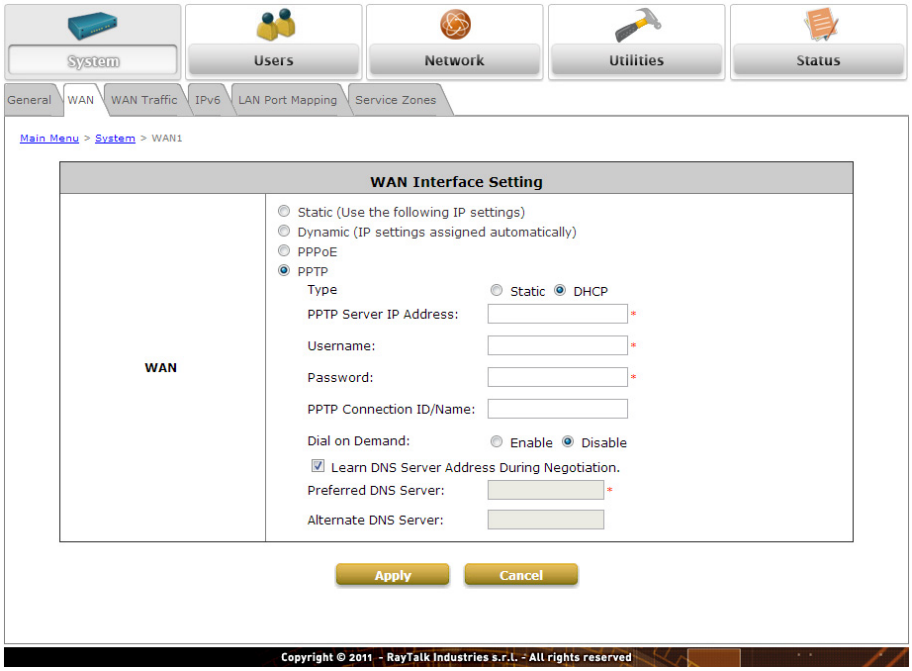
3.2.3 PPPoE

PPPoE: When selecting PPPoE to connect to the network, please set the "Username", "Password", "MTU" and "Clamp MSS". There is a Dialon demand function under PPPoE. If this function is enabled, a Maximum Idle Time slot will be available for inputting a value.When the idle time is reached, the system will automatically disconnect itself.



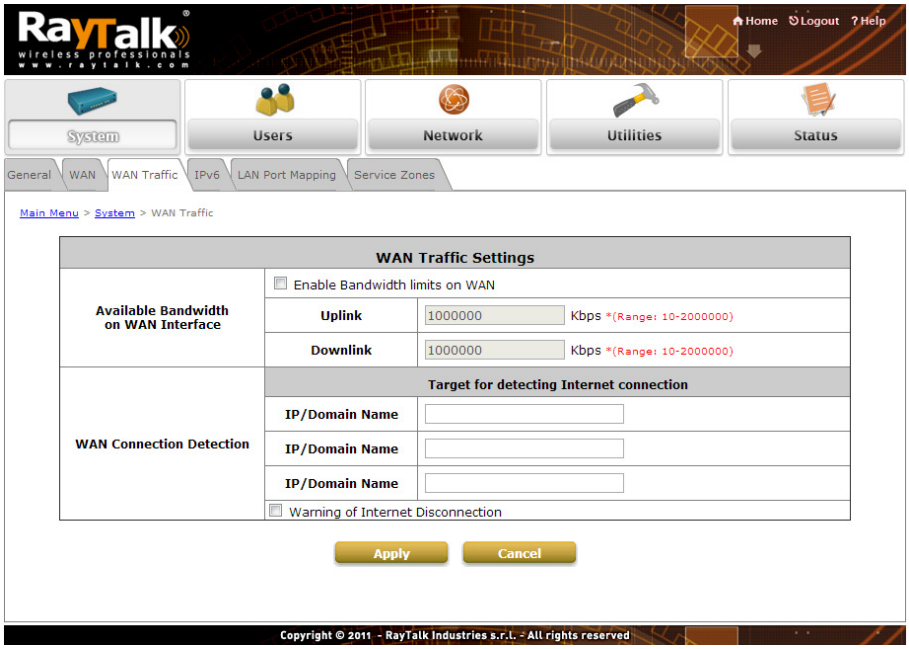
3.2.4 PPTP

PPTP: Although not a popular method, PPTP protocol for dialup connections is adapted by some ISPs (in European Countries). Your PPTP ISP will issue you an account with a password as well as the PPTP server address.



3.3 Internet Connection Detection

To configure Internet Connection Detection, go to: ***System >> WAN Traffic***.



Internet Connection Detection: When this function is enabled, system will try to access these IP/Domain addresses, if system can reach these IP/Domain addresses, it means that the outbound Internet connection is in normal state. On the other hand, there is a textbox available for the administrator to enter a message reminder. This reminder will appear on clients' screens when Internet connection is down.

3.4 WAN Bandwidth Control

To configure WAN Bandwidth Control, go to: ***System >> WAN Traffic***.

The feature gives administrators control over the entire system's traffic on the WAN interface. These parameters set here should not exceed the real bandwidth provided by your ISP. For example, if your xDSL is 8Mbs/640kbs, you may input values equal to or less than the speed here.

Available Bandwidth on WAN Interface:

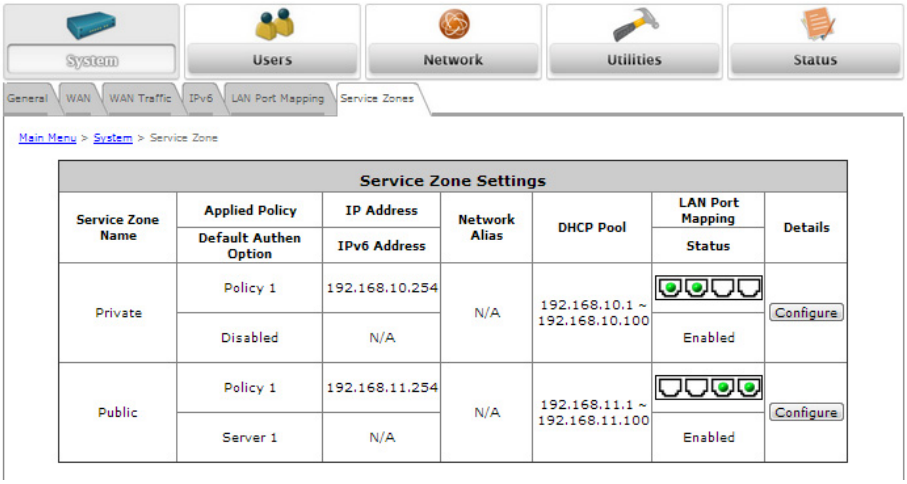
- **Uplink:** It specifies the maximum uplink bandwidth that can be shared by clients of the system.
- **Downlink:** It specifies the maximum downlink bandwidth that can be shared by clients of the system.

3.5 What is Zone

To configure a Zone, go to: ***System >> Service Zones***.

A *Zone* is a logical network area that covers wired or wireless networks, or both of them. By associating it with a unique ESSID of a Zone, wireless network is divided into different logical zones. Clients attempting to access the resources within a Zone will be controlled based on the access control profile of that Zone, such as authentication, security features, wireless encryption methods, traffic control, etc.

There are two Zones that can be utilized by the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 – Private Zone and Public Zone, as shown in the table below. Private Zone means clients are not required to be authenticated before using the network service. However, clients in Public Zone are required to obtain authentication before using the service.



- **Service Zone Name:** Mnemonic name of the Zone.
- **Applied Policy:** Current Policy that is applied to Zone.
- **Default Authen Option:** Default authentication method/server that is used within the Zone.
- **IP/IPv6 address:** Shows the LAN IP address. IPv6 is support and can be configured from the IPv6 tab.
- **Network Alias:** Shows the IP address that bridges to different subnets configured in the Network Alias List.
- **DHCP Pool:** Shows the range of LAN IP address which clients are assigned to get from DHCP.
- **LAN Port Mapping:** Each physical LAN port can be set individually to map to a specific zone, and can be configured from the LAN Port Mapping tab (refer to 3.5.1).
- **Status:** Shows the Private/Public Zone mappings to the physical LAN ports.
- **Details:** Configurable, detailed settings for each Zone.

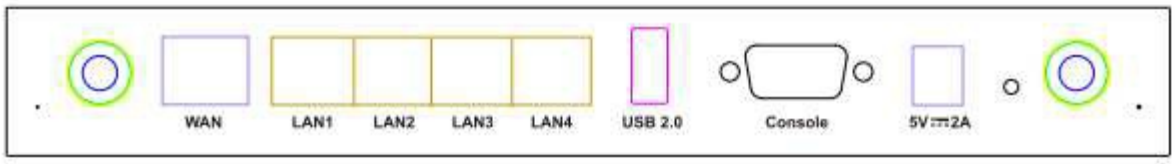
Click the ***Configure*** button to configure each Zone: **Basic Settings**, **Authentication Settings**, **Wireless Settings**, and **WDS Settings (Public Zone only)**.

3.5.1 Port Role Assignment

The MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 supports two zones, Private and Public. In the Private Zone, authentication is not required to access the network, whether it is via wired and wireless connection.

In the Public Zone, the **"Authentication Required for Zone"** option is enabled by default, so clients have to be authenticated successfully before surfing the Internet.

The Zone and Port mappings are shown below, LAN1, LAN2 maps to Private Zone and LAN3, LAN4 to Public Zone respectively.



Note:

System's WMI can also be accesses via WAN port as long as the administrator uses an IP address listed on the **Management IP Address List** (Go to *System >> General >> Management IP Address List*). If both WAN and LAN ports are unable to reach the WMI, please use console interface to resolve this issue.

3.5.2 Planning Your Internet Network

MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 supports two zones, Private and Public. In the Private Zone, authentication is not required to access the internet via wired and wireless.

In Public Zone, by default the **"Authentication Required for Zone"** option is enabled, so clients are required to be authenticated successfully before surfing the Internet. Administrator can access the Web Management Interface (WMI) of the RAYTALK RA-696 through the wired LAN port.

3.5.3 Configure Zone Network

To configure Zone network; go to: System >> *Service Zone.* Click the button *Configure* for Private zone for further configuration.

The parameter descriptions of Basic Settings for Private Zone and Public Zone are the same. The wireless settings under each zone will be covered in the next section.

➢ Network Interface:

- Operation Mode: Contains NAT mode and Router mode. When NAT mode is chosen, service zone runs in NAT mode. When Router mode is chosen, this zone runs in Router mode.
- IP Address: The IP Address of this zone.
- Subnet Mask: The subnet Mask of this zone.

➢ DHCP Server: Related information needed for setting up the DHCP Server is listed here.

To further configure the DHCP Server, click the button ***Configure***.

Please note that when "*Enable DHCP Relay"* is enabled, the IP address of clients will be assigned by an external DHCP server.

The system will only relay DHCP information from the external DHCP server to downstream clients of this zone.

- **Start IP Address / End IP Address:** A range of IP addresses that the built-in DHCP server will assign to clients.
  Note: please change the Management IP Address List accordingly (at *System >> General >> Management IP Address List*) to permit the administrator to access the RAYTALK RA-696 admin page after the default IP address of the network interface is changed.
- **Preferred DNS Server:** The primary DNS server that is used by this Zone.
- **Alternate DNS Server:** The substitute DNS server that is used by this Zone.
- **Domain Name:** Enter the domain name for this zone.
- **WINS Server:** The IP address of the WINS (Windows Internet Naming Service) server if WINS server is applicable to this zone.
- **Lease Time:** This is the time period when the IP addresses issued from the DHCP server will be valid and available.
- **Reserved IP Address List:** Each zone can reserve up to 40 IP addresses from
- predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. The administrator can reserve a specific IP address for a special device with a certain MAC address.

4 Let Your Network Be a Wireless Network

4.1 System Wireless General Settings

To configure System's Wireless General Settings, go to: ***System >> Service Zones.*** Click the button ***Configure*** for ***Private zone*** for further configuration.

Wireless General Settings	
Band	802.11g+802.11n ▼ Pure 11n
Short Preamble	(•) Enable ( ) Disable
Short Guard Interval	(•) Enable ( ) Disable
Channel Width	20 MHz ▼
Channel	1 ▼
Max Transmit Rate	Auto ▼
Transmit Power	Highest ▼
DTIM Period	1 (1-255ms)
ACK Timeout	100 (0-255ms)

Wireless General Settings:

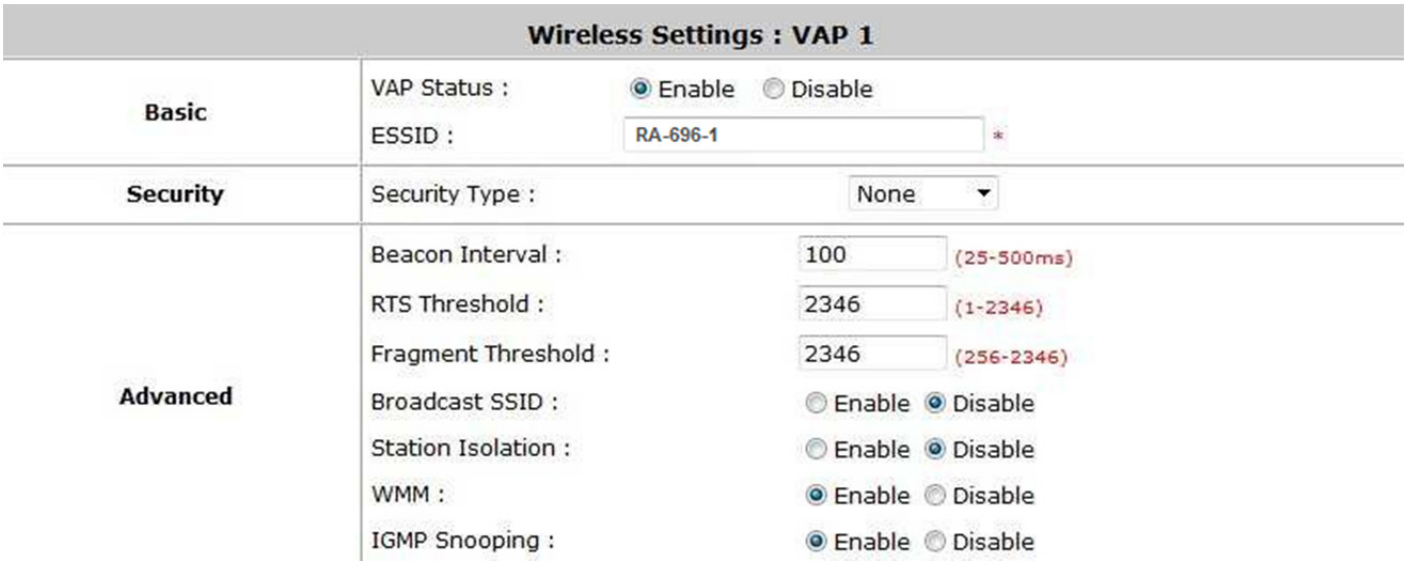
- **Band:** There are 4 modes to select, **802.11b** (2.4G, 1~11Mbps), **802.11g** (2.4G, 54Mbps), **802.11b+g**, and **802.11g+n**. Otherwise the administrator could enable the 'Pure 11n' to only utilize the 11n band.
- **Short Preamble:** The length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Select **Enable** for **Short Preamble** or **Disable** for **Long Preamble**.
- **Short Guard Interval (802.11g+n only):** The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. With 802.11n, short guard interval is half of what it is used to be to increase throughput. Select **Enable** to use Short Guard Interval or *Disable* to use normal Guard Interval.
- **Channel Width (802.11g+n only):** For 802.11n, doubling channel bandwidth to 40 MHz is supported to enhance throughput.
- **Channel:** Select the appropriate channel from the drop-down menu to correspond with your network settings, for example, Channel 1-11 is available in North American and Channel 1-13 in Europe, or choose the default *Auto*.
- **Max Transmit Rate:** The default is **Auto**. Available range is from 1 to 300 Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **Transmit Power:** Keep the default setting, or select from range to make the Access Point use different transmit power as you wish.
- **DTIM Period:** Input the DTIM Interval that is generated within the periodic beacon at a specified frequency. Higher DTIM will let the wireless client save energy, but the throughput will be decreased/worsened.
- **ACK Timeout:** The time interval for waiting for the "acknowledgement (ACK) frame". If the ACK is not received within the interval then the packet will be re-transmitted. Higher ACK Timeout interval will decrease the packet lost, but the throughput will be decreased/worsened.

4.2 Zone Wireless Settings

Each zone has its own VAP and corresponds to one SSID. In Private zone, it's VAP1 and the SSID is hidden, so public users cannot scan this SSID in the air, for privilege users who already know this SSID, they can manually associate to the SSID of Private zone. On the other hand, the SSID of VAP2 under Public zone by default is enabled with SSID Broadcast feature, allowing public users to scan this SSID in the air.

After wireless general settings are done, use the parameters in Wireless Settings under zone configuration to fine tune the wireless network under Private and Public Zone.

To configure Private Zone's Wireless Settings, go to: ***System >> Service Zone***, click **Configure** for Private zone



➢ **Wireless Settings: VAP1 (Wireless Settings Private Zone)**

- **Basic:** Enable the VAP Status if you wish to provide wireless service under this zone. Assign an ESSID to VAP1 under Private Zone or use the default, the ESSID of Private Zone will not be broadcast and internal staff will need to associate to Private Zone's VAP1 manually.
- **Security:** Configure the wireless network under Private Zone with security encryption to prevent unauthorized wireless association if necessary. The supported encryption standards are WEP and WPA-PSK.
- **Advanced:** The parameters in Advanced are wireless settings that allow customization of data transmission, enhanced security and wireless roaming.

  Beacon Interval: The entered amount of time indicates how often the beacon signal will be sent from the VAP. The default value is set at 100 ms.

  RTS Threshold: Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the frame to prevent hidden node problems. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the RAYTALK RA-696 or in areas where the clients are far apart and can detect only the RAYTALK RA-696 but not each other. The default value is set at 2346.

  Fragment Threshold: Enter a value between 256 and 2346. The default value is 2346. Packet size larger than this threshold, will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

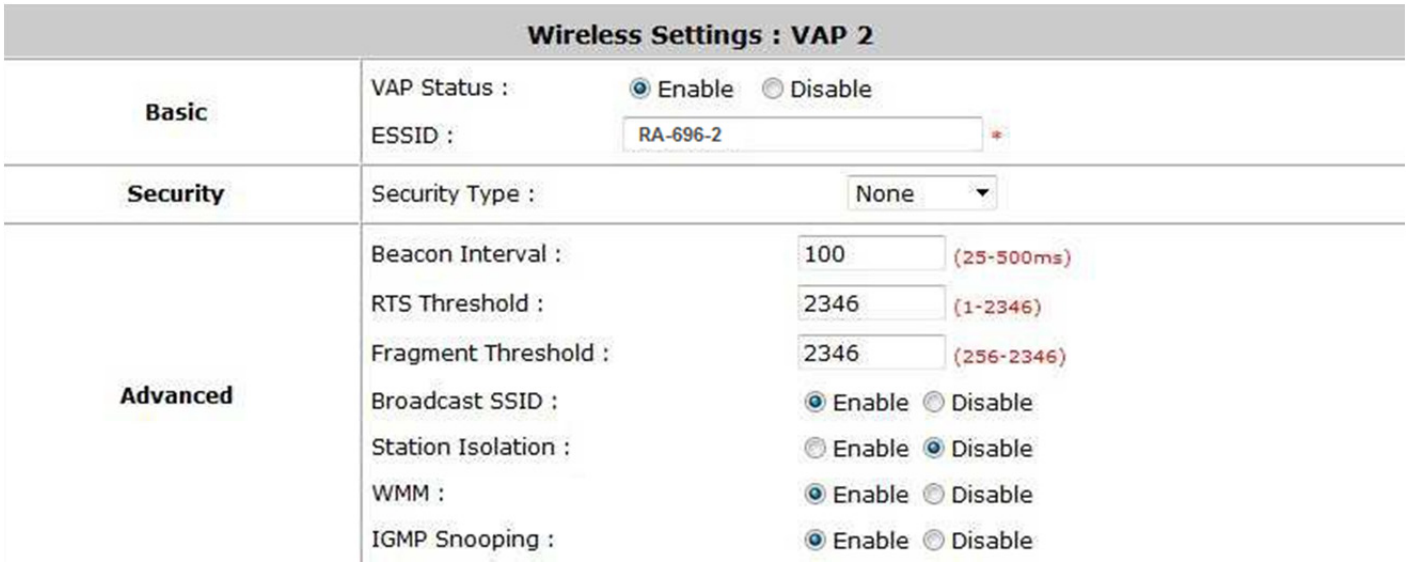
Broadcast SSID: The administrator has the option of enabling or disabling the SSID for VAP1 which is the Private Zone. Default value is set at Disable where users will not be able to scan for the SSID.

Station Isolation: By enabling this function, all stations wirelessly associated to this zone are isolated from one another and can only communicate with the system.

WMM: The default is *Enable.* Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.

IGMP Snooping: IGMP is a multicast constraining mechanism which may flood the broadcast domain. This is effective for dense internet usage such as conventions or campuses.

Normally, we use VAP2, the VAP under Public Zone, to provide wireless service to public clients in a hotspot environment. To configure Public Zone's Wireless Settings, go to: ***System >> Service Zones***, click **Configure** for Public zone.



➢ **Wireless Settings: VAP2 (Wireless Settings for Public Zone)**

- **Basic:** Enable the VAP Status if you wish to provide wireless service under this zone. Assign an ESSID for VAP2 under Public Zone or use default, the ESSID of Public Zone will be broadcasted in default settings to allow it to be scanned in the air.
- **Security:** Configure the wireless network under Public Zone with security encryption to prevent unauthorized wireless association if necessary. The encryption standards supported are WEP and WPA-PSK.
- **Advanced:** The parameters in Advanced are wireless settings that allow customization of data transmission, enhanced security and wireless roaming.

  Beacon Interval: The entered amount of time indicates how often the beacon signal will be sent from the VAP. The default value is set at 100 ms.

  RTS Threshold: Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the frame to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the RAYTALK RA-696 or in areas where the clients are far apart and can detect only the RAYTALK RA-696 but not each other. The default value is set at 2346.

Fragment Threshold: Enter a value between 256 and 2346. The default value is 2346.

A packet size larger than this threshold will be fragmented (sent with several pieces instead of one chunk) before transmission.

A smaller value results in smaller frames but allows a larger number of frames in transmission.

A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

Broadcast SSID: Enable to broadcast VAP2's SSID in the air, Disable to hide VAP's SSID so that it cannot be scanned.

Station Isolation: By enabling this function, all stations wirelessly associated to this zone are isolated from one another and can only communicate with the system.

WMM: The default is *Enable.* Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background.

Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than that of voice and video.

Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority.

This option works with WMM-capable clients only.

IGMP Snooping: IGMP is a multicast constraining mechanism which may flood the broadcast domain. This is effective for dense internet usage such as conventions or campuses.

4.3 Zone Wireless Security

To configure Zone Wireless Security, go to: ***System >> Service Zones***, click ***Configure*** for Private zone or click ***Configure*** for Public zone.

After the above configurations are finished, setting up the wireless security is very important to protect your wireless network.

Wireless Settings : VAP 1		
Basic	VAP Status :	◉ Enable ○ Disable
	ESSID :	RA-696-1 *
Security	Security Type :	None
Advanced	Beacon Interval :	100 (25-500ms)
	RTS Threshold :	2346 (1-2346)
	Fragment Threshold :	2346 (256-2346)
	Broadcast SSID :	○ Enable ◉ Disable
	Station Isolation :	○ Enable ◉ Disable
	WMM :	◉ Enable ○ Disable
	IGMP Snooping :	◉ Enable ○ Disable

Wireless Settings : VAP 2		
Basic	VAP Status :	◉ Enable ○ Disable
	ESSID :	RA-696-2 *
Security	Security Type :	None
Advanced	Beacon Interval :	100 (25-500ms)
	RTS Threshold :	2346 (1-2346)
	Fragment Threshold :	2346 (256-2346)
	Broadcast SSID :	◉ Enable ○ Disable
	Station Isolation :	○ Enable ◉ Disable
	WMM :	◉ Enable ○ Disable
	IGMP Snooping :	◉ Enable ○ Disable

- **Security:**

For each zone, administrators can set up the wireless security profile, it includes **WEP** and **WPA-PSK**.

➢ **WEP:**

- **802.11 Authentication:** Select from **Open System** or **Shared Key**.
- **WEP Key Length:** Select from **64-bit**, **128-bit**, **152-bit** key length.
- **WEP Key Format:** Select from **ASCII** or **Hex** format for the WEP key.
- **WEP Key Index:** Select a key index from **1~4**. The WEP key index is a number that specifies which

WEP key will be used for the encryption of wireless frames during data transmission.

- **WEP Keys:** Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.

➢ **WPA-PSK:**

- **Cipher Suite:** Select an encryption method from **TKIP (WPA)**, **AES (WAP2)**, or **Mixed**.
- **Pre-shared Key / Pass-phrase:** Enter the key value for the pre-shared key or pass-phrase.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.

4.4 Wireless Layer 2 firewall

Go to **Network >> Layer 2 Firewall**

The system provides an additional security feature, Layer2 Firewall, in addition to the standard wireless security.

Layer2 Firewall offers a firewall function that is tailored specifically for Layer2 traffic, providing another choice of shield against possible security threats coming from/going to WLAN (AP interfaces); hence, besides firewall policies configured in Policies, this extra security feature will assist to mitigate possible security breach.

This section provides information in the following functions: **Generic Firewall Rules**, **Predefined and Custom Service Protocols** and **Advanced**.

4.4.1 Generic Firewall Rules

You can choose to enable or disable the wireless Generic Firewall. This section provides an overview of firewall rules for the system's wireless interface; 6 default rules with up to a total 20 firewall rules are available for configuration.

Firewall Rules						
No.	**Active**	**Action**	**Rule Name**	**Ether Type**	**Remark**	**Operation**
1	☑	Block	CDP	IEEE 802.3		Edit Move to Insert Before Delete
2	☑	Block	STP	IEEE 802.3		Edit Move to Insert Before Delete
3	☑	Block	GARP	IEEE 802.3		Edit Move to Insert Before Delete
4	☑	Block	RIP	IPv4		Edit Move to Insert Before Delete
5	☑	Block	HSRP	IPv4		Edit Move to Insert Before Delete
6	☑	Block	OSPF	IPv4		Edit Move to Insert Before Delete
7	☐	Block	rule 7	ANY		Edit Move to Insert Before Delete
8	☐	Block	rule 8	ANY		Edit Move to Insert Before Delete
9	☐	Block	rule 9	ANY		Edit Move to Insert Before Delete
10	☐	Block	rule 10	ANY		Edit Move to Insert Before Delete

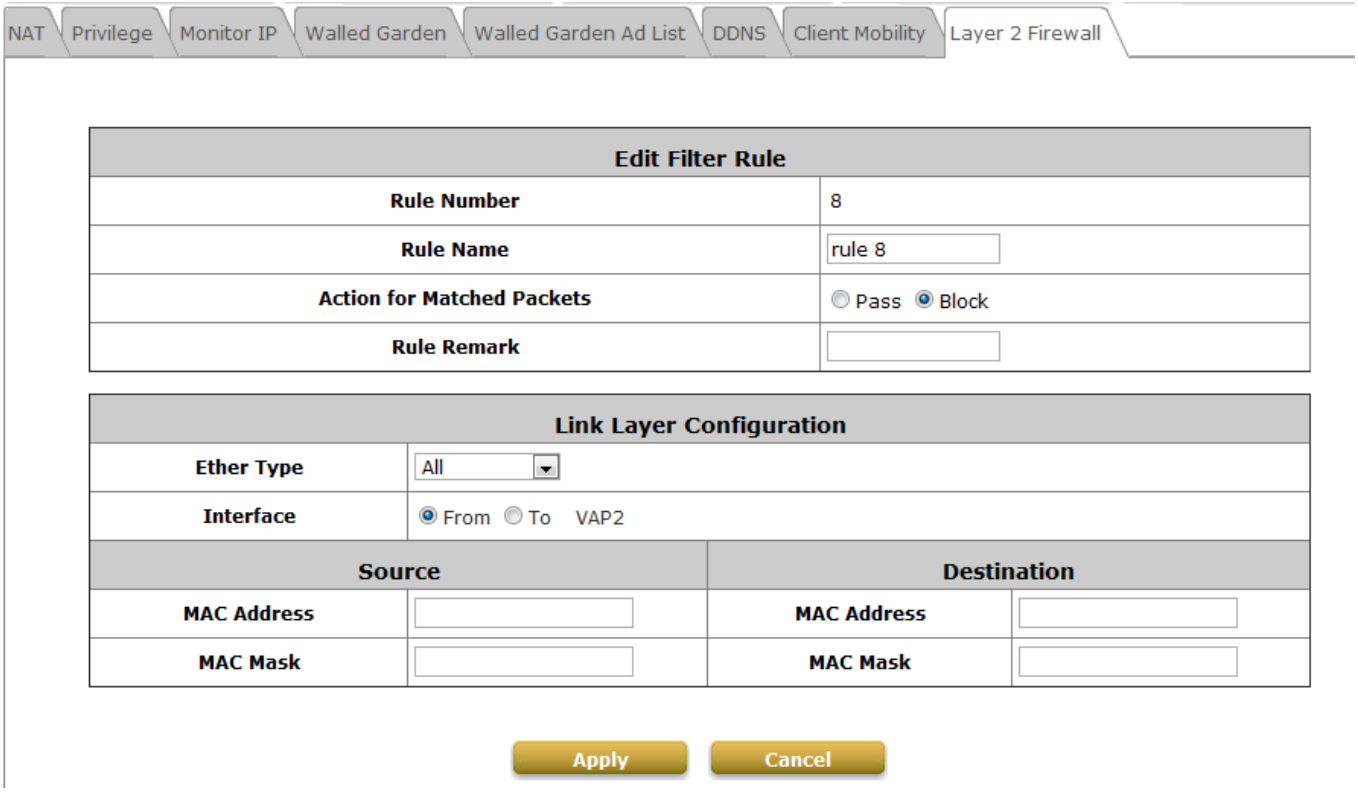
(Total:10) First Prev Next Last

From the overview table, each rule is designated with the following field;

- **No.:** The numbering will decide the priority of which the system will carry out the available firewall rules in the tables.
- **Active:** Checking this field will mark the rule as active which means this rule will be enforced.
- **Action: Block** denotes a block rule; **PASS** denotes a pass rule.
- **Rule Name:** This is the denominated name of the rule.
- **EtherType:** It denotes the type of traffic subjected to this rule.
- **Remark:** It shows the additional reference information of this rule.
- **Operation:** 4 actions are available; ***Edit*** denotes to edit the rule details, ***Move to*** denotes to move the rule to a specified rule number, ***Insert Before*** denotes to insert a rule before the current rule, and ***Delete*** denotes to delete the rule.

>>To edit a specific rule,

Edit in **Operation** column of firewall rules will lead to the following page for detailed configuration. On this page, the rule can be edited from an existing rule for revision.



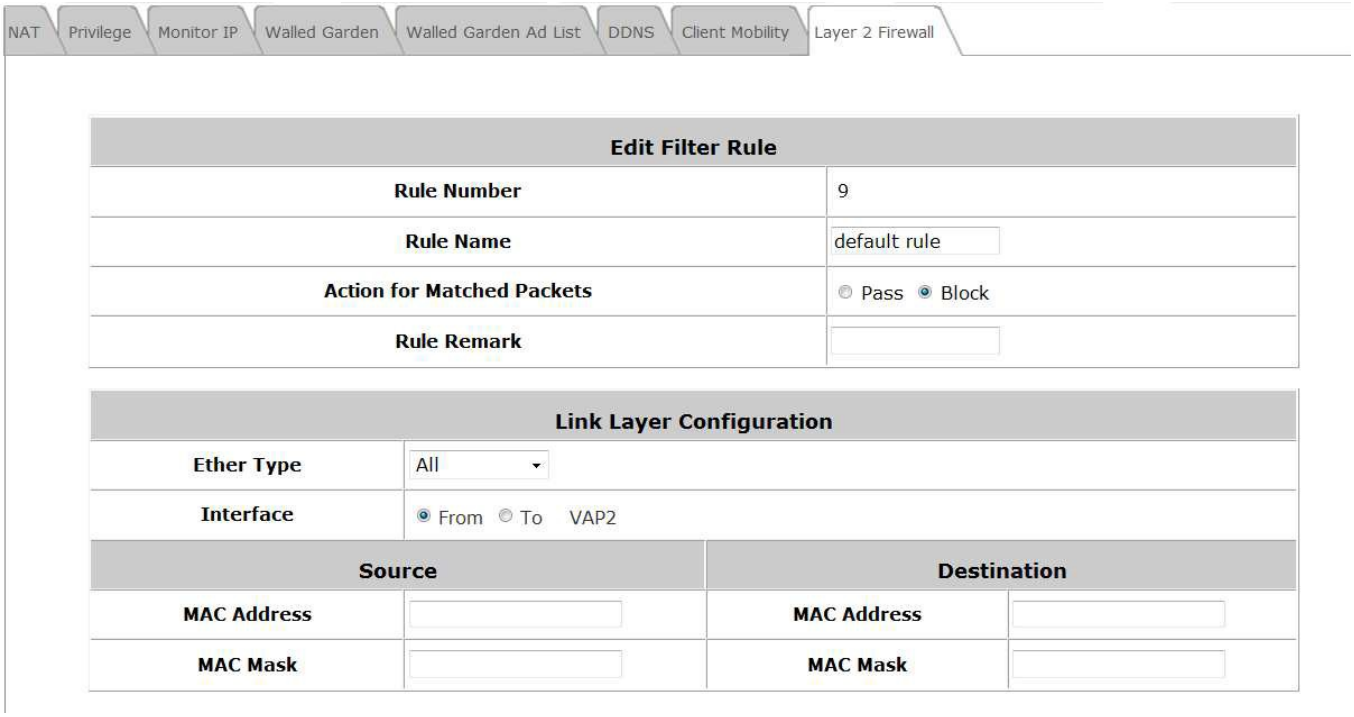
- **Rule Number:** The numbering of this specific rule will decide its priority among available firewall rules on the list.
- **Rule name:** The rule name can be denominated here.
- **Action for Matched Packets:** The rule can be chosen to be **Block** or **Pass** packets that match the rule criteria.
- **Rule Remark:** The additional reference note of this rule can be specified here.
- **EtherType:** The drop-down list will provide the available types of traffics subject to this rule.
- **Interface:** For specifying the traffic direction (To or From VAP2) subjected to this rule.
- **IPv4 Service** (when EtherType is **IPv4**)**:** Select the available upper layer protocols/services from the drop-down list.
- **DSAP/SSAP** (when EtherType is **IEEE 802.3**): The value can be further specified for the fields in 802.2 LLC frame header.
- **SNAP Type** (when EtherType is **IEEE802.3**)**:** The field can be used to indicate the type of encapsulated traffics.
- **Opcode** (when EtherType is **ARP**)**:** This list can be used to specify the ARP Opcode in ARP header.
- **Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields (when EtherType is **ARP**).

- **Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields (when EtherType is **ARP**).

When the configurations are made; please click ***Apply*** to let the firewall rule take effort.

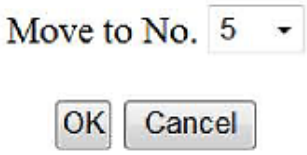
>>To insert a specific rule,

Inserting Before in **Operation** column of firewall list will lead to the following page for detailed configuration with a rule ID for the rule currently being inserted.

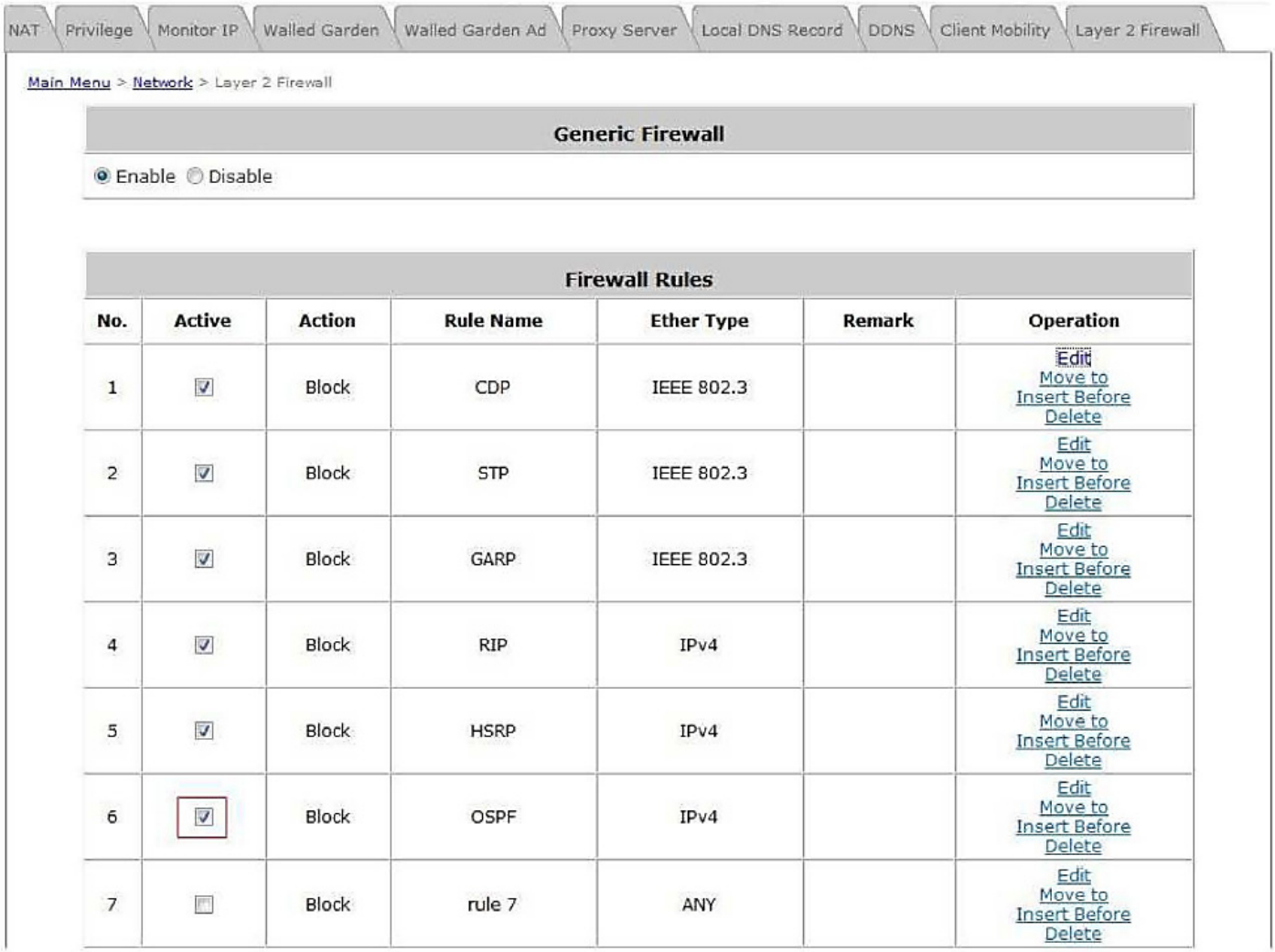


>>To move a specific rule,

Move to in **Operation** column of firewall rules will lead to the following page for reordering confirmation. Click ***OK*** to save the changes made.



Please make sure all the desired rules are checked as Active and click the Apply button below on the overview page.

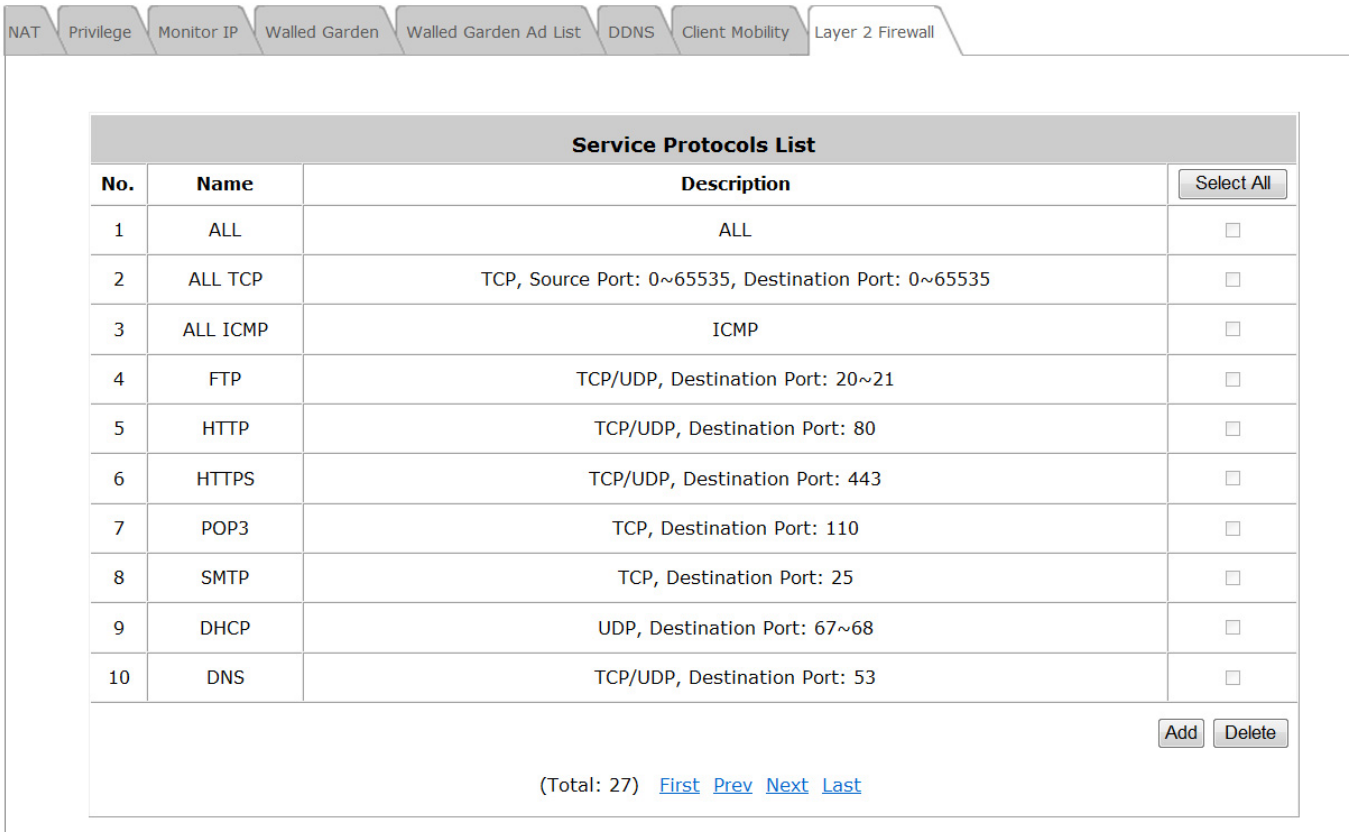

NAT
Privilege
Monitor IP
Walled Garden
Walled Garden Ad
Proxy Server
Local DNS Record
DDNS
Client Mobility
Layer 2 Firewall
Main Menu > Network > Layer 2 Firewall
Generic Firewall
Enable
Disable
Firewall Rules
No.
Active
Action
Rule Name
Ether Type
Remark
Operation
1 Block CDP IEEE 802.3 Edit Move to Insert Before Delete
2 Block STP IEEE 802.3 Edit Move to Insert Before Delete
3 Block GARP IEEE 802.3 Edit Move to Insert Before Delete
4 Block RIP IPv4 Edit Move to Insert Before Delete
5 Block HSRP IPv4 Edit Move to Insert Before Delete
6 Block OSPF IPv4 Edit Move to Insert Before Delete
7 Block rule 7 ANY Edit Move to Insert Before Delete

4.4.2 Predefined and Custom Service Protocols

The administrator can add or delete firewall service protocols here; the services on this list will become available drop-down options to choose from in firewall rule (when EtherType is IPv4).

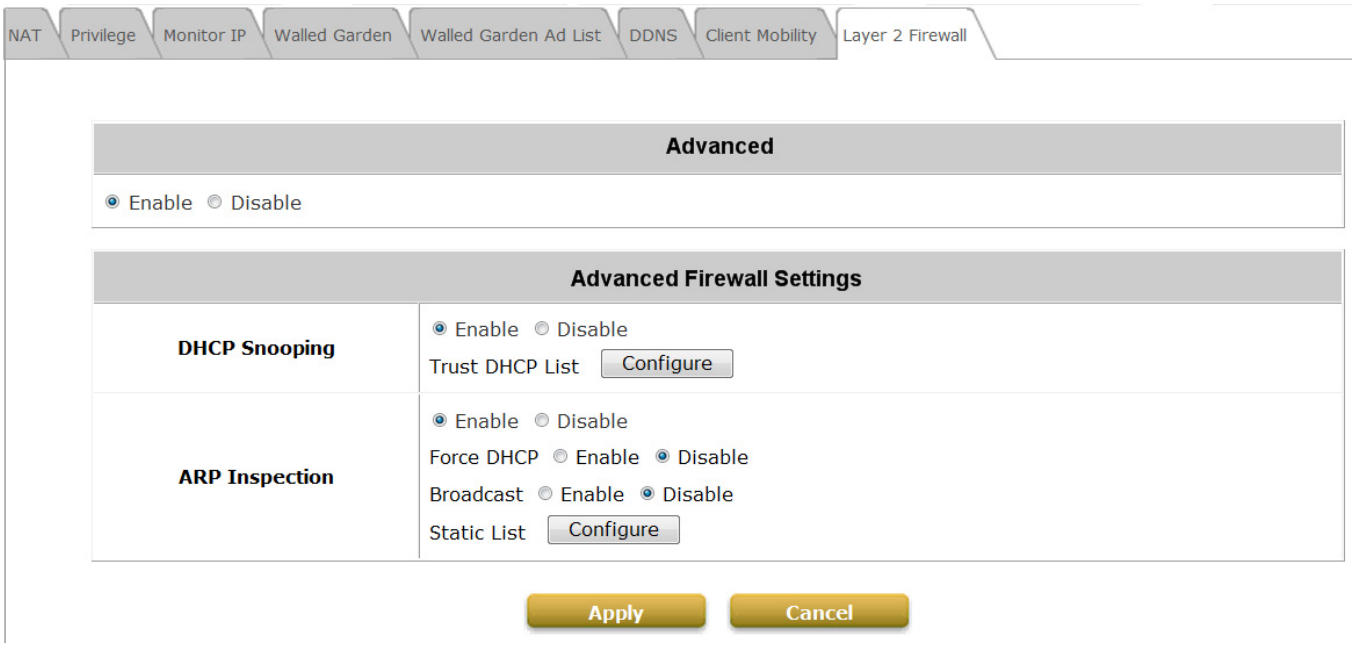
The first 27 entries are default services and the administrator can add any extra desired services.

These 27 default firewall services cannot be deleted but can be disabled.



4.4.3 Advanced

Advanced Firewall Settings can be enabled to supplement the firewall rules, providing extra security enhancement against DHCP and ARP traffics traversing the available interfaces of the system.



- **DHCP Snooping**: When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack. In addition, the **Trusted DHCP List** (IP/MAC) can be used to specify legitimate DHCP servers to prevent rouge DHCP server.
- **ARP Inspection**: When enabled, ARP packets will be validated against ARP spoofing.
    - **Force DHCP** option when enabled, the AP only learns MAC/IP pair information through DHCP packets. Since devices configured with static IP address does not send DHCP traffic, any client with static IP address will be blocked from internet access unless its MAC/IP pair is listed and enabled on the **Static List.**
    - **Broadcast** can be enabled to let other AP (with L2 firewall feature) learn the trusted MAC/IP
    - pairs to issue ARP requests.
    - **Static List** can be used to add MAC or MAC/IP pairs of devices that are trusted to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears on the static list (with different MAC), their ARP requests will be dropped to prevent eavesdropping.

If any settings are made, please click ***Apply*** to save the configuration before leaving this page.

5 Who Can Access the Network

5.1 Type of Users

To configure Users, go to: ***Users >> Authentication***.

This section is for administrators to pre-configure authentication servers for the entire system. Concurrently up to three servers can be selected and pre-configured for static user authentication. One server uses built-in LOCAL database while the other two servers use external RADIUS database. In addition, 'ONDEMAND' server can be configured for temporary user authentication.

Authentication Settings		
Auth Option	**Auth Database**	**Postfix**
Server 1	LOCAL	local
Server 2	RADIUS	radius1
Server 3	RADIUS	radius2
On-demand User	ONDEMAND	ondemand
FREE	FREE	N/A

- **Authentication Settings:** There are four different authentication options in MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 that use databases: **LOCAL**, **RADIUS1**, **RADIUS2**, **ONDEMAND** and **FREE. Local** and **On-demand** are built in databases with user credentials stored locally, and **RADIUS** is one of the most common external authentication databases. **FREE** is an access option that allows users to access networks with any specified identity token on the login page. Click on the Authentication Options to configure.
- **Auth Option:** Set a name for the authentication databases by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_), space and dot (.) only. This name is used for the administrator to easily identify the authentication options such as HQ-RADIUS.
- **Postfix**: A postfix represents the authentication server in a complete username. For example, **user1@local** means that this user (user1) will be authenticated by the LOCAL authentication database.
- **Black List:** There are 5 sets of black lists provided by the system. A user account listed on the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one (or None) black list from the drop-down menu and it will be applied to this specific authentication option.
- **Configure:** Click the ***Configure*** button to edit a specific authentication database for the server. For example, if you want to edit the *Local* authentication database, please click the ***Configure*** button for **Local**.

5.1.1 Local

Click the button ***Configure*** for **Local** for further configuration.

Local User Database Settings	
Local User List	
Account Roaming Out	○ Enable ◉ Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	○ Enable ◉ Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)

- **Local User List:** It allows the administrator to view, add or delete local user accounts. The ***Upload User*** button is for importing a list of user accounts from a text file. The ***Download User*** button is for exporting all local user accounts into a text file. Clicking the hyperlink of a user account leads to a page for configuration.

Add User: Click this button to enter the **Adding User(s) to the List** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC Address"**, **"Remark" and login "Schedule"**. Select a desired **Group** to classify local users. Click ***Apply*** to complete adding the user(s).

MAC address of a networking device can be bound with a local user as well.

It means this user must log in to the system with a networking device (namely PC) that has the corresponding MAC address.

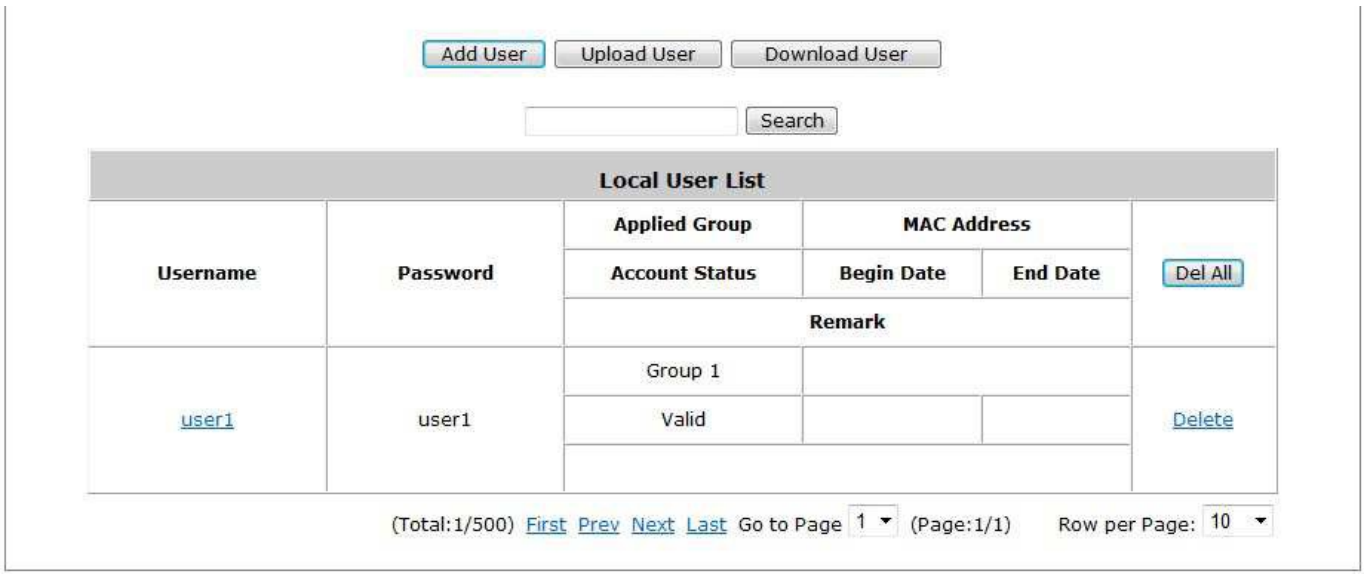
That is, this user cannot log in with other networking devices.

An expiration time can be enabled for the user.

Adding User(s) to the List

No.	Username*	Password*	MAC Address (XX:XX:XX:XX:XX:XX)	Group	Remark	Begin Date	End Date	Enable Expire Time
1				Group 1		Select	Select	
2				Group 1		Select	Select	
3				Group 1		Select	Select	
4				Group 1		Select	Select	
5				Group 1		Select	Select	
6				Group 1		Select	Select	
7				Group 1		Select	Select	
8				Group 1		Select	Select	

- ***Search*:** Enter a keyword of a username or remark to be searched in the text file and click this button to perform the search. All usernames matching the keyword will be listed.



- ***Del All***: Click this button to delete all the users at once or click Delete (hyperlinked) to delete a specific user individually.

Edit User: If in need of editing, click the desired user account on **Local User List** to enter the **User Profile** Interface for that particular user, and then modify or add information such as *Username*, *Password*, *MAC Address* (optional), *Applied Group* (optional) and *Remark* (optional).

An expiration time can be Enabled and the Begin/End.

Date can be selected. Click *Apply* to complete the modification.

Main Menu > Users > Authentication > Option > Local > local User List > Editing User

Editing Existing User Data

5.1.2 RADIUS

There are two RADIUS authentication databases for configuration.

Click ***Configure*** for any one of **RADIUS** servers for further configuration.

The RADIUS server sets the external authentication for user accounts.

Enter the information concerning the primary server and/or the secondary server (the secondary server is not mandatory).

The fields with red asterisks are necessary information.

These settings will become effective immediately after clicking ***Apply.***

External RADIUS Server Related Settings			
802.1X Authentication	○ Enable ◉ Disable		
Username Format	◉ Leave Unmodified ○ Complete (e.g. user1@postfix) ○ Only ID (e.g. user1)		
NAS Identifier			
NAS Port Type	19 *(Default 19, Range: 0~35)		
Accounting Delay Time	0 *(Deafult: 0)		
Service Type	1 *(Default: 1, Range: 1~11)		
Class-Group Mapping	Configure		
DM & CoA Settings	Configure		
Acct Interim for users' IP changed	○ Enable ◉ Disable (Acct Interim is sent when users' IP are chagned if Enable)		
Failover between RADIUS Servers	○ Enable ◉ Disable		
Attributes Priority	Follow Server's Setting		
	Standard RADIUS Attributes		
	Session Timeout	240 Minutes *(Range: 5-1440 mins)	
	Idle Timeout	10 Minutes *(Range: 1-120 mins)	
	Acct Interim Interval	15 Minutes *(Range: 1~120 mins, 0 is disable)	
	WISPr Vendor Specific Attributes		
	Redirection URL		
	Billing Class Of Service		
	Session Terminate on Billing Time	○ Enable ◉ Disable	
	Session Terminate Time	Never	
	Bandwidth Setting	Group 1	
Retransmission Settings	Number of Retries	3 *(Default: 3)	
	Timeout	6 *(Default: 6)	
Primary RADIUS Server			
Authentication Server	*(Domain Name/IP Address)		
Authentication Port	*(Default: 1812)		
Authentication Secret Key	*		
Authentication Protocol	CHAP		
Accounting Service	◉ Enable ○ Disable		
Accounting Server	*(Domain Name/IP Address)		
Accounting Port	*(Default: 1813)		
Accounting Secret Key	*		
Secondary RADIUS Server			
Authentication Server	(Domain Name/IP Address)		
Authentication Port			
Authentication Secret Key			
Authentication Protocol	CHAP		
Accounting Service	◉ Enable ○ Disable		
Accounting Server	(Domain Name/IP Address)		
Accounting Port			
Accounting Secret Key			

➢ **External RADIUS Related Settings**

- **802.1X Authentication:** Enable /Disable 802.1X authentication for users authenticated through this Server.
- **Username Format:** Select the format of the user login information required to be sent to the external RADIUS Server. You may choose to send username in **Complete** (userID + Postfix), **Only ID** or **Leave Unmodified**. Please note that if Leave Unmodified option is selected, the system will send the input as is.
- **NAS Identifier:** This attribute is the string identifying the NAS originating the access request. System will send this value to the external RADIUS server, if the external RADIUS server needs this.
- **NAS Port Type:** Indicates the type of physical port the network access server is using to authenticate the user. System will send this value to the external RADIUS server, if the external RADIUS server needs this.
- **Account Delay Time:** This attribute adds flexibility for the RAYTALK RA-696 to process accounting requests in the time specified. Default is set at 0.
- **Service Type:** This attribute indicates the type of service the user has requested or the type of service to be provided, required for some RADIUS servers that only accepts specified service types.
- **Class-Group Mapping:** This function is to impose a Group on a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes log into the system via the RADIUS server, each client will be mapped to an assigned Group.

RADIUS Group Mapping - Server 2

○ Enable ◉ Disable

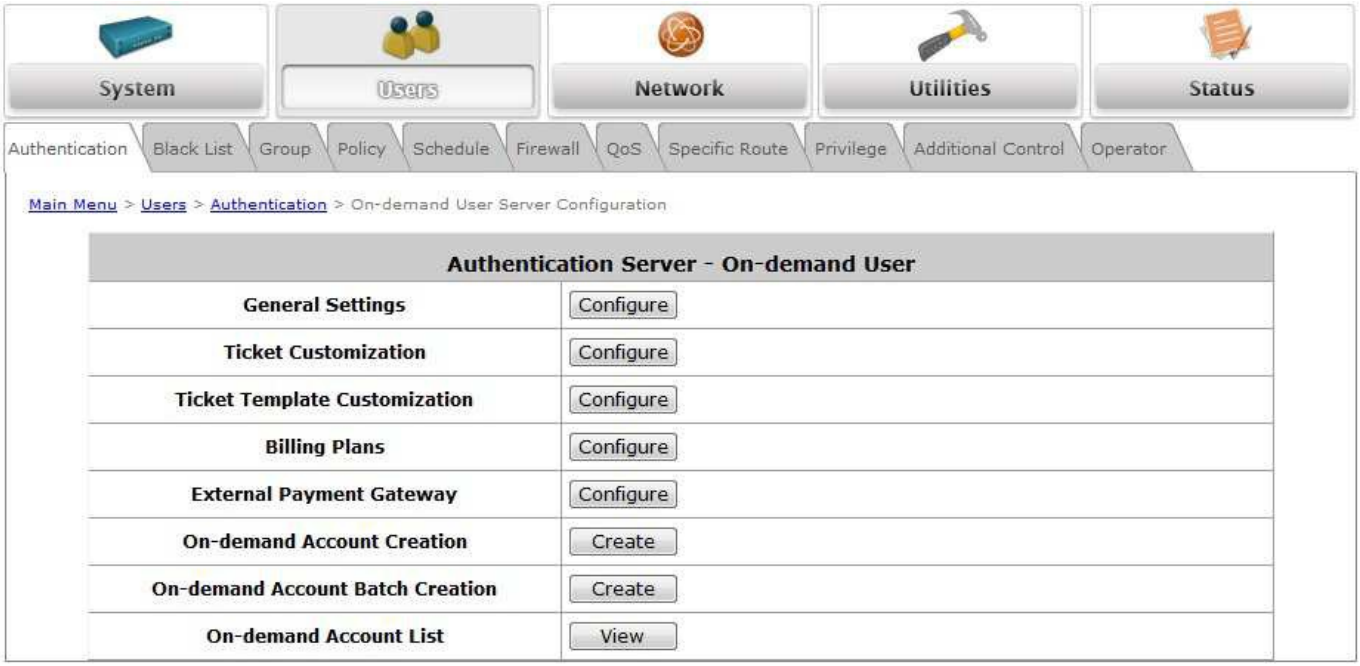
No.	Class Attribute Value	Group	Remark
1		Group 1	
2		Group 1	
3		Group 1	
4		Group 1	
5		Group 1	

- **DM & CoA Settings:** This function allows administrator to assign users to receive Disconnect Messages / Change of Authorization from the server and sessions can be terminated instantly. Click Configure to enter the IP addresses of the users.
- **Attributes Priority:** This section shows the Standard RADIUS attributes which include Session Timeout, Idle Timeout and Acct Interim Interval; and WISPr Vendor Specific Attributes. These attributes are predetermined, and if needed, choose Overwrite Server's Setting to make changes.

- **Primary / Secondary RADIUS Server**
  - **Authentication Server:** Enter the domain name or IP address of your RADIUS Server.
  - **Authentication Port:** Enter the Port number used for authentication.
  - **Accounting Port:** Enter the Port number used for accounting.
  - **Authentication Secret Key:** Secret Key used for authentication.
  - **Accounting Service:** Enable / Disable RADIUS accounting.
  - **Accounting Server:** Enter the domain name or IP of your accounting server
  - **Authentication Protocol:** Select Challenge-Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).
  - **Accounting Secret Key:** The key between the RADIUS server and the gateway to test the authenticity of the link.

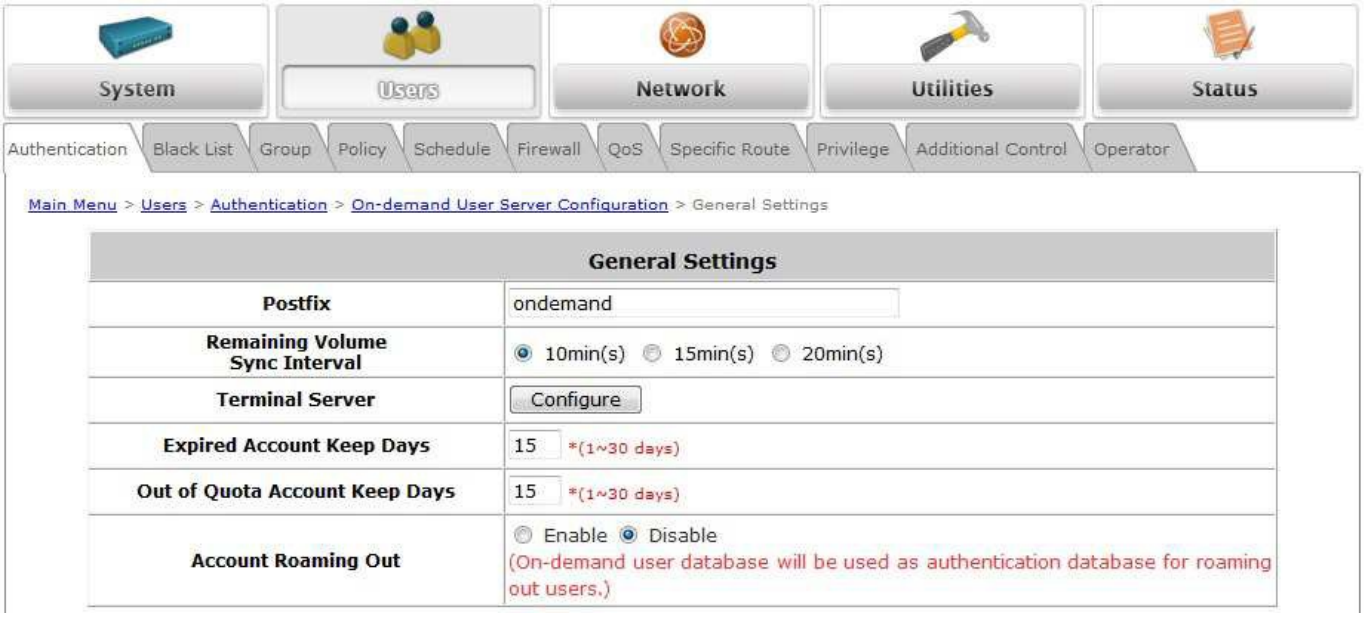
5.1.3 On-Demand User

On-demand User Server Configuration: The administrator can configure this authentication method to create on-demand user accounts. This function is designed for hotspot owners to provide temporary users with free or paid wireless Internet access in the hotspot environment. Major functions include accounts creation, users monitoring list, billing plan and external payment gateway support.



1) **General Settings**

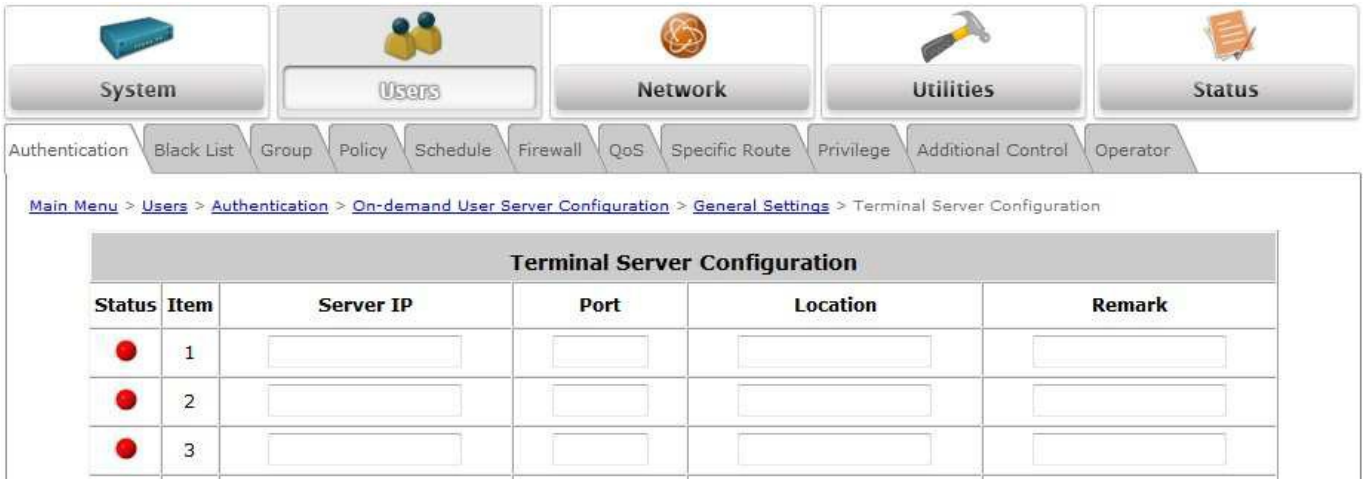
This is the common setting for the On-demand User authentication option.



- **Postfix:** The string of characters needed to be entered with the username during login.
- **Remaining Volume Sync Interval:** Select a desired interval for on-demand user quota update. The quota information, i.e. remaining time or remaining quota displayed on the on-demand user login success page will be refreshed according to the time interval configured here.

- **Terminal Server:** Terminal Server Configuration is a list of serial-to-Ethernet devices that communicate with the system only; there is no need to go online or go through authentication process.

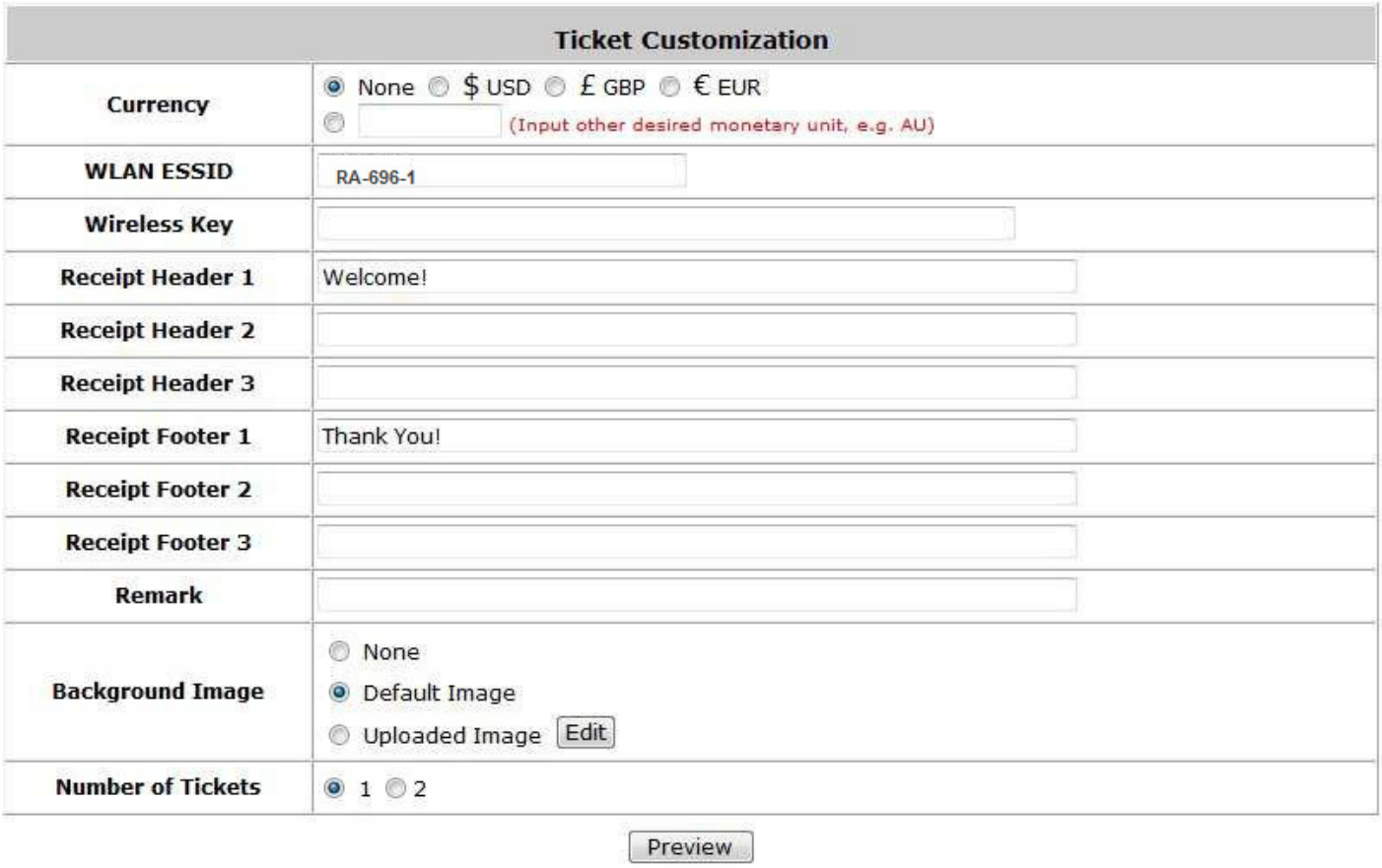
Enter the device IP and the port number into the respective fields.



- **Account Roaming Out:** When Account Roaming Out is enabled, a link will be available to define the client device authorized to roam by entering the IP address, Subnet Mask, and Secret Key.

2) Ticket Customization

On-demand account ticket can be customized here and previewed on the screen.



- **Currency:** Select the desired currency unit for charged internet access.
- **WLAN ESSID:** The entered name will be the ESSID of the Public Zone.

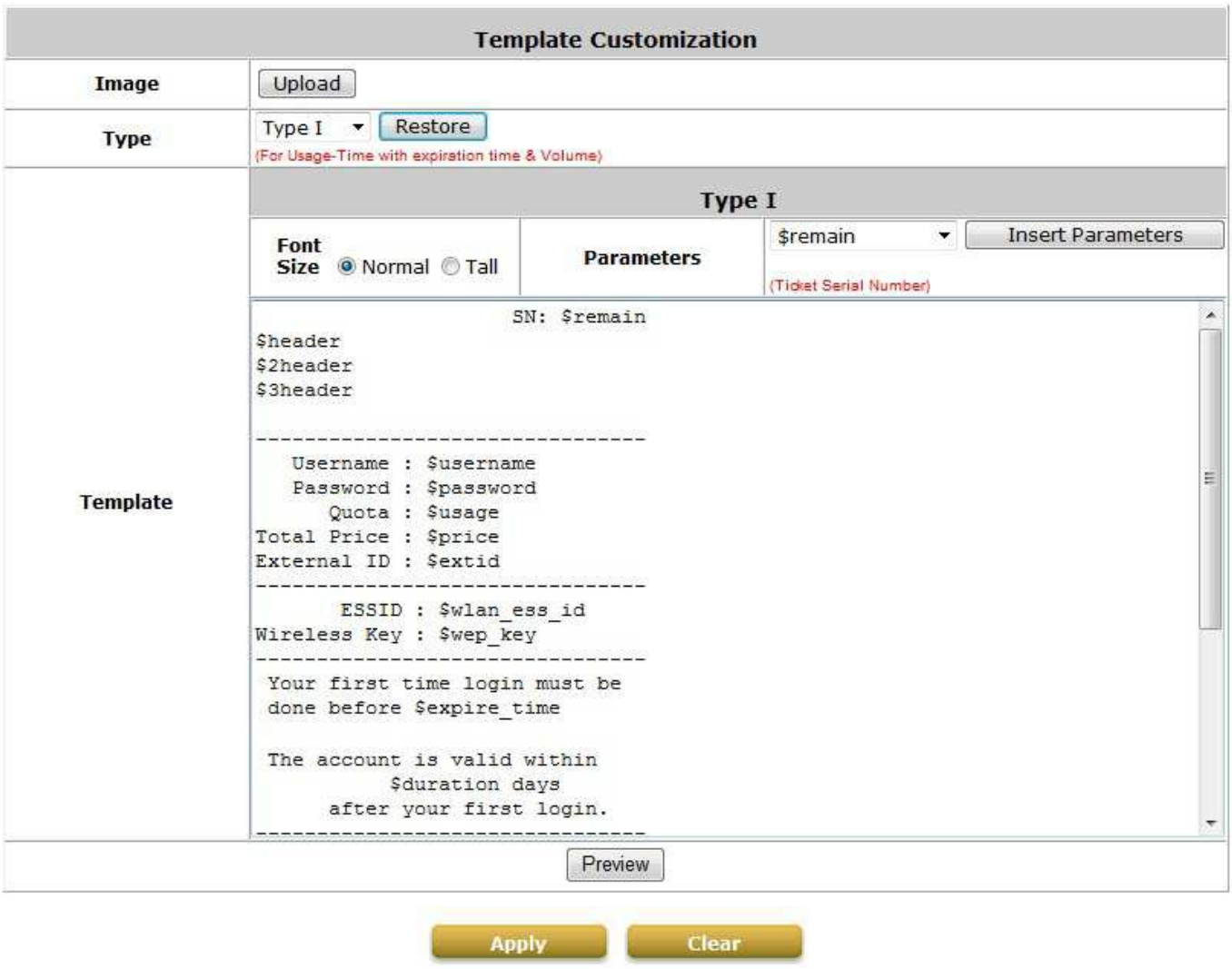
- **Wireless Key:** The wireless key configured in Public Zone Settings will be shown.
- **Receipt Header(Optional):** There are 3 receipt headers supported by the system. The entered content will be printed on the receipt.
- **Receipt Footer(Optional):** There are 3 receipt footers supported by the system. The entered content will be printed on the receipt.
- **Remark:** Enter additional information that will appear at the bottom of the receipt.
- **Background Image:** You can choose to customize the ticket by uploading your own background image for the ticket, or choose none. Click **Edit** to select the image file and then click **Upload**.

The background image file size limit is 100 Kbytes. No limit for the dimensions of the image is set, but a 460x480 image is recommended.

- **Number of Tickets:** Enable this function to print duplicate receipts. Another Remark field will appear when the Number of Ticket is selected to 2 and the content will appear at the bottom of the 2nd duplicate receipt.
- **Preview:** Click ***Preview***, the ticket will be shown, including the information of username and password with the selected background. You can also print the ticket here.

3) Ticket Template Customization

Administrators can customize contents on the On-demand tickets using this template.



4) Billing Plans

Administrators can configure several billing plans. Click the ***Edit*** button to enter the page of **Editing Billing Plan**.

Configure billing plans with desired account type, expiration date, price, etc. Click ***Apply*** to save the plan.

Go back to the screen of **Billing Plans**, check the ***Enable*** checkbox or click **Select all** , and then click **Apply**, the plan(s) will be activated.

Billing Plans

Plan	Account Type	Quota	Price	Enable	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	2.99	☑	Group 1	Edit
2	Duration-time	Valid for 4 hour(s) elapsed time	4.99	☑	Group 2	Edit
3	Volume	100 Mbyte(s) of traffic volume quota	1.99	☑	Group 3	Edit
4	Hotel Cut-off-time	Valid until 23:00 the following day	3.99	☑	Group 4	Edit
5	N/A			☐	Group 1	Edit
6	N/A			☐	Group 1	Edit
7	N/A			☐	Group 1	Edit
8	N/A			☐	Group 1	Edit
9	N/A			☐	Group 1	Edit
0	N/A			☐	Group 1	Edit

- **Plan**: The number of the specific plan.
- **Type**: This is the type of plan, based on which it defines how the account can be used including Usage-time, Volume, Hotel Cut-off and Duration-time.
- **Quota**: The limit on how On-demand users are allowed to access the network.
- **Price**: The unit price charged for buying an account from this billing plan.
- **Enable**: Check the checkbox to activate the plan.
- **Group**: Users under this billing plan will be classified under this group. The default value is Group 1.
- **Function**: Click the *Edit* button to add one billing plan. For detailed information regarding on-demand accounts and billing plan configuration, please refer to ***Appendix E, On-demand Account types & Billing Plan***.

5) External Payment Gateway

This section is for merchants to set up an external payment gateway to accept payments in order to provide wireless access service for end customers who wish to pay for the service online.

The options are **Authorize.Net**, **PayPal**, **SecurePay**, **WorldPay** or **Disable**. For detailed parameter descriptions please refer to ***Appendix F, External Payment Gateways.***

External Payment Gateway

Authorize.Net	PayPal	SecurePay	WorldPay	Disable
○	○	○	○	◉

6) On-demand Account Creation

After at least one billing plan is enabled, the administrator can generate single on-demand user accounts here.

Click this to enter the On-demand Account Creation page.

Click ***Create*** from the desired plan to create an on-demand account.

The username and password of to-be-created on-demand account is configurable. Select ***Manual created*** in Username/Password Creation and administrator can enter a desired username and password for the on-demand account.

In addition, an External ID such as student's school ID can be entered together with account creation.

After the account is created, you can click ***Printout*** to print a receipt which will contain the on-demand user's information, including the username and password. Moreover, you can click ***Send to POS*** to print a receipt by a POS device.

Note:

If no Billing plan is enabled, accounts cannot be created by clicking ***Create***.
Please go back to Billing Plans to activate at least one Billing plan by clicking ***Edit*** and ***Apply*** the setting to activate the plan. The printer used by ***Print*** is a pre-configured printer connected to the administrator's computer.

On-demand Account Creation

Plan	Account Type	Quota	Price	Status	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create
5	N/A	N/A	N/A	Disabled	Create
6	N/A	N/A	N/A	Disabled	Create
7	N/A	N/A	N/A	Disabled	Create
8	N/A	N/A	N/A	Disabled	Create
9	N/A	N/A	N/A	Disabled	Create
0	N/A	N/A	N/A	Disabled	Create

- **Plan**: The number of a specific plan.
- **Account Type**: Show account type of the plan in Usage-time. Duration-time or Hotel Cut-off.
- **Quota**: The total amount of time, interval or traffic volume for On-demand users to access the network.

For Time users, it is the total time. For Volume users, it is the total amount of traffic.

- **Price**: For each plan, this is the unit price charged for an account.
- **Status**: Show the status in enabled or disabled.
- **Function**: Press Create for the desired plan; and 'Creating an On-demand Account' will appear for creation.

On-demand Account Creation					
Plan	Account Type	Quota	Price	Status	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Hotel Cut-off-time	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create

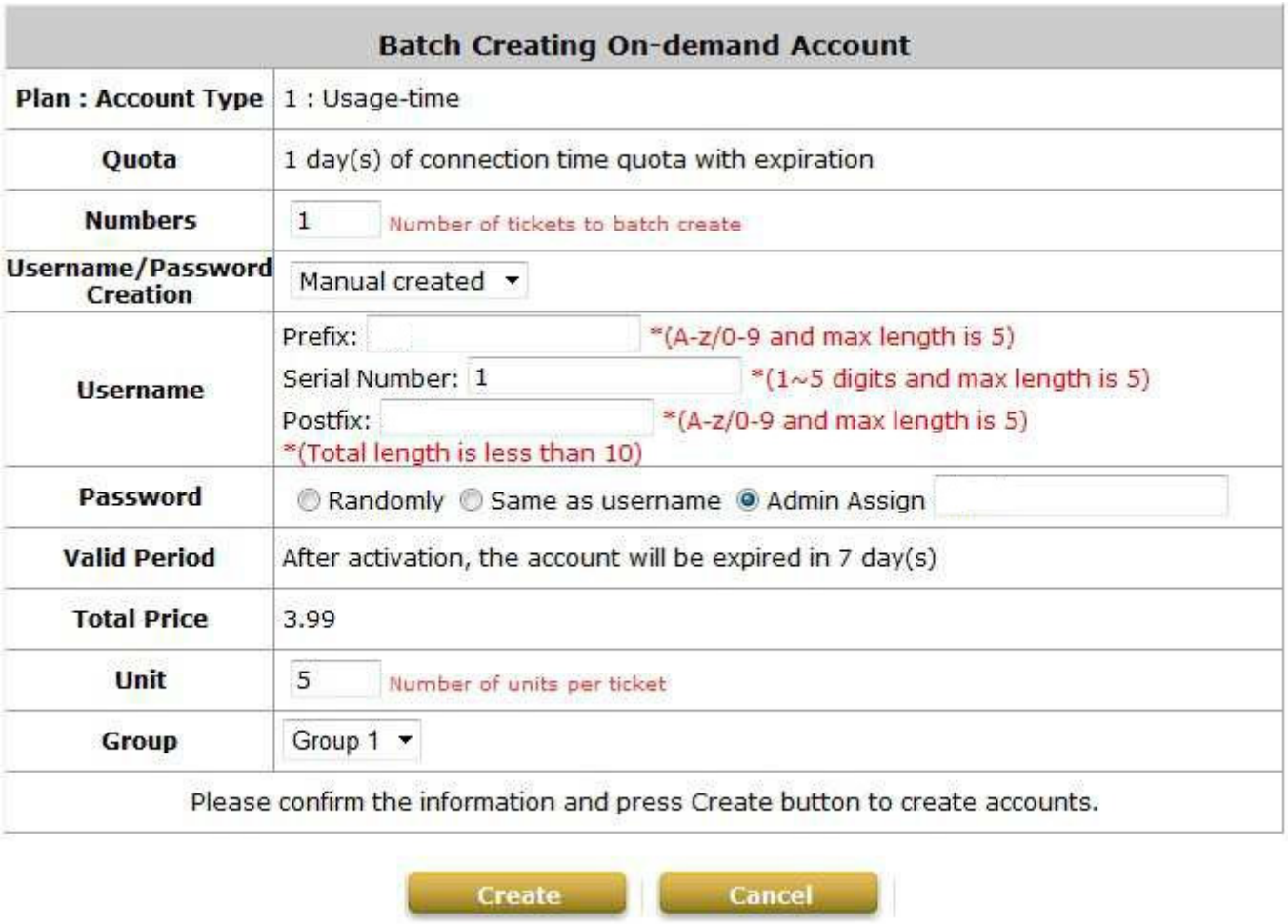
Creating an On-demand Account	
Plan : Account Type	2 : Usage-time
Quota	11 min(s) of connection time quota
Account Creation	System created
Account Activation	First time login must be done within 1 hour(s)
Total Price	1
Unit	1 Units per ticket
Group	Group 1
Reference	Add a reference related to this account (for example, the customer's name)
External ID	Enter an external ID such as Library ID No.
Please confirm the information and press Create button to create an account.	

Create Cancel

7) On-demand Account Batch Creation

After at least one billing plan is enabled, the administrator can generate multiple on-demand user accounts at once with batch creation.

For potential hotspot operators who may wish to pre-generate guest accounts for sale, On-demand feature has a batch create functionality which allows the administrator or operator with access authority to On-demand page, to create multiple accounts for an enabled billing plan in batch, and send them to POS printer for generating physical ticket printout for sale.



- **Account Type:** Show account type of the plan in Usage-time, Duration-time or Hotel Cut-off.
- **Quota:** The total amount of time, interval or traffic volume for On-demand users to access the network.
- **Numbers:** The desired number of accounts to be created from the plan.
- **Username/Password Creation:** Usernames and passwords can be created randomly by system or self-created by administrator.
- **Username:** To manually create a username, the Prefix and Postfix can be chosen. The serial number increases at single increments when batch accounts are created.
- **Password:** Passwords are customizable and can be created randomly by system or self-created by administrator.
- **Valid Period:** Shows when the account will expire.
- **Total Price:** For each plan, this is the unit price charged for an account.
- **Unit:** Number of units of Quota per ticket
- **Group:** On-demand users can be allocated to a defined User Group when On-demand accounts are created.

The generated accounts may be downloaded for safe keeping, or sent to printer for batch printout.

8) On-demand Account Creation by Quick Button

The **Quick Button** located on the front panel of RAYTALK RA696 is a quick On-demand account generation button. This button is designed to create On-demand accounts without the need to enter WMI. There should be a serial POS printer like RT-TP5x5 which is directly connected to the console port of RAYTALK RA696.

When the administrator has properly connected a RT-TP5x5 printer to the console port, pressing this button will generate an On-demand account using billing plan no.1 and print out the account credentials via the POS printer.

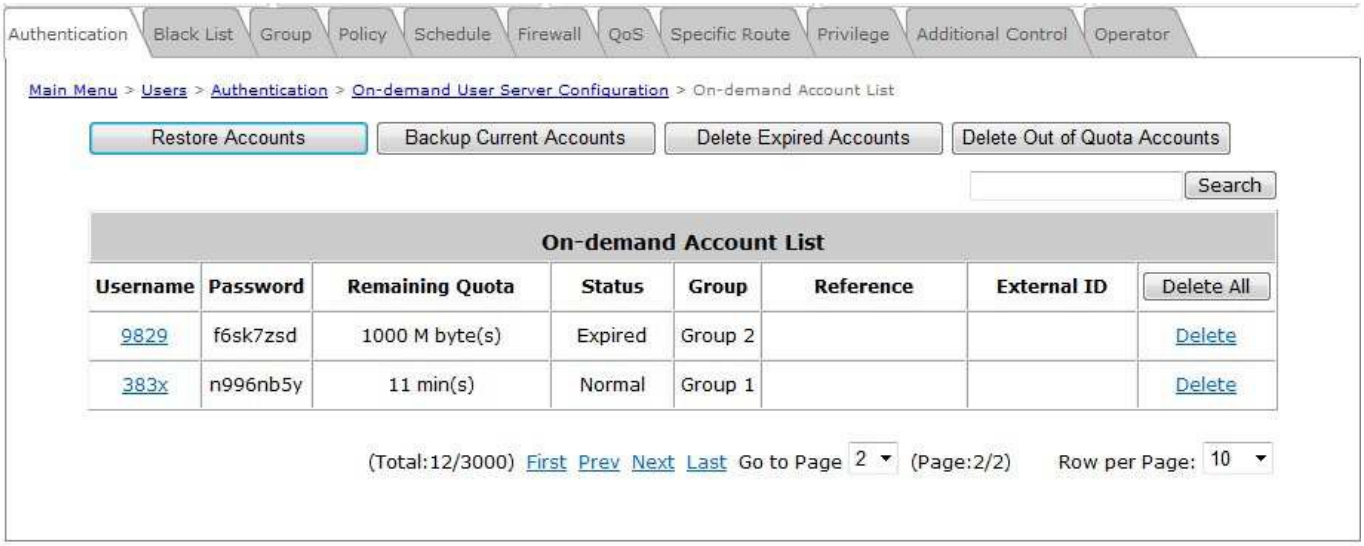
Please note that the corresponding billing plan no. for this **Quick Print** button is always billing plan 1.

Should the network administrator wish to configure different account types for generation, please modify billing plan no.1.

**Only supports normal font for ticket customization.*

9) On-demand Account List

All created On-demand accounts are listed and related information is also provided.



- **Search:** Enter a keyword of a username, External ID, or reference, to be searched in the text file and click this button to perform the search. All usernames, External ID, or reference, matching the keyword will be listed.
- **Username:** The login name of the account.
- **Password:** The login password of the account.
- **Remaining Quota:** The remaining time or volume, or the cut-off time that the account can continue to use to access the network.
- **Status:** The status of the account.
  - **Normal:** the account is not currently in use and has not exceeded the quota limit.
  - **Online:** the account is currently in use.
  - **Expired:** the account is not valid any more, even if there is remaining quota left.
  - **Out of Quota:** the account has exceeded the quota limit.
  - **Redeemed:** the account has been applied for account renewal.
  - **External ID:** This is an additional information field combined with a unique account, for example the customer's name or social security number etc.
  - **Reference:** Any other additional information, for example venue where the account is generated etc.
  - **Delete All:** This will delete all the users at once.
  - **Delete:** This will delete the users individually.

10) **Redeem On-demand Accounts**

Hello, you are logged in via 3p6z@ondemand
To log out, please click the "Logout" button.
Login time: 2009-06-02 11:11
Remaining Time:
4 Hour 59 Min 51 Sec
Redeem
Logout

For Usage-time accounts, when the remaining quota is insufficient or if they are running out of quota, they can use the redeem function to extend their quota.

After the user has got, or bought a new account, they just need to click the **Redeem** button in the login success page to enter Redeem Page, input the new account **Username** and **Password** and then click **Enter**.

This new account's quota will be extended to the original account. However, the Redeem function can only be used with the same billing type, i.e. Volume accounts can only be redeemed with another Volume account and so on.

Note:

The maximum quota is 364dys 23hrs 59mins 59secs" even after redemption. If the redeemed amount exceeds this number, the system will automatically reject the redemption process.

Duration-time and Hotel Cut-off type do not support redemption function.

5.1.4 Free Authentication

When the Free Authentication option is **Enabled**, users will have an option of logging in with an email address without authentication.

This can be activated under Service Zone Settings configurations.

The constraints can be set specifically with the mapped Group profile. MAC addresses will be checked to avoid malicious use of free access.

When Trial Account is Enabled, Administrator can choose to set the Usage Time and Refresh Time.

The server remembers the MAC address of the user.

Hence the user can only get a new Free authentication account after the refresh time has been reached.

5.2 User Login

5.2.1 Default Authentication

There are different types of authentication databases (LOCAL, RADIUS and ONDEMAND) that are supported by the system.

But authentication can only be set in the Public Zone.

A postfix is used to inform the system which authentication option is to be used for authenticating an account (e.g. Bob@local or Tim@radius1 etc.) when multiple options are concurrently in use.

One of the authentication options can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "local" is the postfix of the default option, then user with username Bob can login as "Bob" without the need to type in "Bob@local".

	Auth Option	Auth Database	Postfix	Default	Enable
Authentication Options	Server 1	LOCAL	local	◉	☑
	Server 2	RADIUS	radius1	○	☑
	Server 3	RADIUS	radius2	○	☑
	On-demand User	ONDEMAND	ondemand	○	☑
	FREE	FREE	N/A	○	☐

5.2.2 Login with Postfix

For each authentication option, set a postfix that is easy to distinguish (e.g. Local) users according to different authentication servers. The acceptable characters are numbers (0~9), alphabet (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

Beside the users managed by Default Authentication, all the other ones with different servers should log into the system with usernames containing postfixes to identify which authentication option they belong to.

The postfix can be set for each Authentication database by clicking the Auth Option.

5.2.3 An Example of User Login

Normally, users will be authenticated before they get network access through MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696. This section presents the basic authentication process of end users.

Please make sure that the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 is configured properly and the network related settings are done.

1. Connect a client PC to Public Zone of MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696. Open an Internet browser and try to connect to any website (in this example, we try to connect to www.google.com).

a) The default user login page will appear in the browser.

2. Enter the username and password (for example, we use a local user account: **test@local** here) and then click ***Login.***

If the ***Remember Me*** checkbox is checked, the browser will store the username and the password on the current computer in order to automatically login to the system at the next login. Then, click the ***Login*** button.

The ***Remaining*** button on the **User Login Page** is for on-demand users only; this is where they can check their Remaining quota.

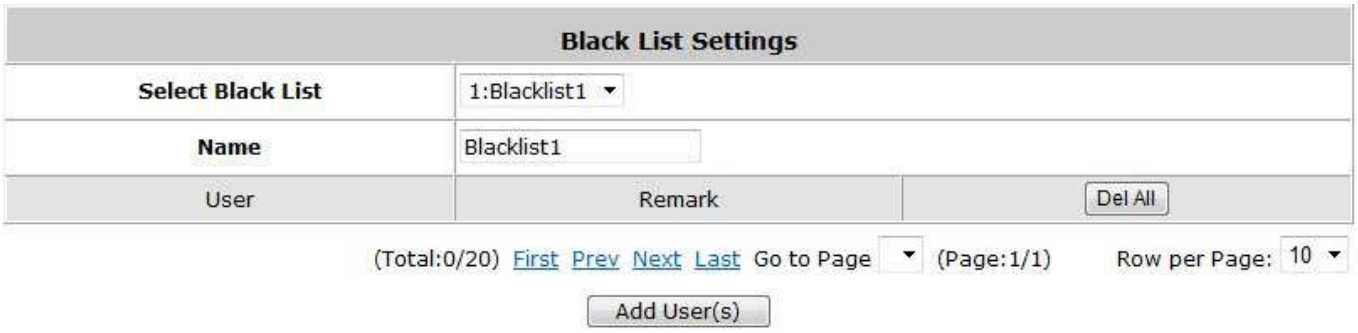
3. Successful! The **Login Success Page** indicates that you are connected to the network and the Internet now!

6 Restrain the Users

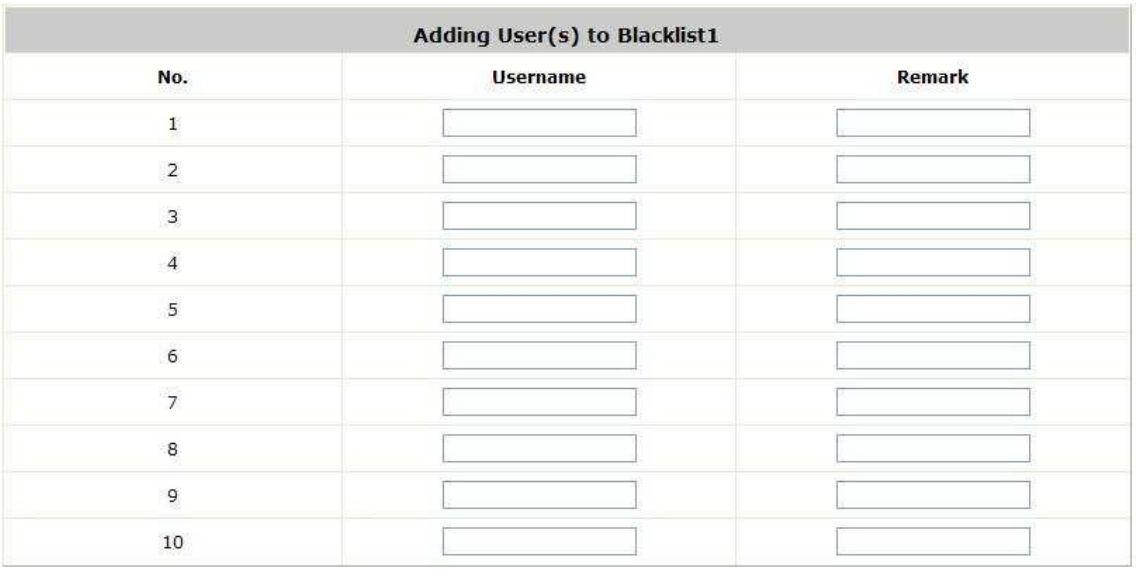
6.1 Black List

To configure Black List, go to: ***Users >> Black List***.

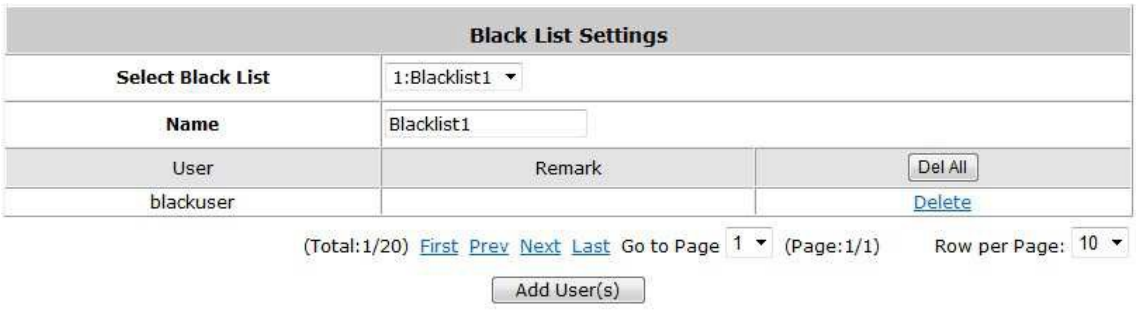
The administrator can add, delete, or edit the black list for user access control. User accounts that appear on the black list will be denied of network access. The administrator can use the pull-down menu to select the desired black list.



- **Select Black List:** There are 5 black list profiles available for utilization.
- **Name:** Set the black list name and it will show on the pull-down menu above.
- **Add User(s):** Click the ***Add User(s)*** button to add users to the selected black list.



After entering the usernames in the **"Username"** field and the related information in the **"Remark"** blank (not required), click ***Apply*** to add the users. If a user needs to be removed from the black list, click the user's **"Delete"** button and or use click ***Del All*** button to remove all users from the black list.



After the Black List editing is completed. You can select the Black List in each Authentication Server to make the list effective.

6.2 Group

To configure Group, go to: ***Users >> Group***.

Users on the RAYTALK RA-696 can be classified into different groups, which can be assigned different Policies and Schedules.

The RAYTALK RA-696 supports up to 5 user Groups.

Group Configuration - Group 1			
Select Group	Group 1		
Group Name	Group 1		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Zone Name	**Enabled**	**Time Span 1** Schedule 1	**Time Span 2** Schedule 1
Service Zone : Private	☑	Policy 1	Policy 1
Service Zone : Public	☑	Policy 1	Policy 1

When the type of authentication database is **RADIUS**, the **Class-Group Mapping** function will be available to allow the administrator to assign a Group for a RADIUS class attribute; therefore, a Group will be mapped to a user of a RADIUS class attribute.

6.3 Policy

To configure Policy, go to: ***Users >> Policy***.

The RAYTALK RA-696 supports multiple Policies, including one **Global Policy** and 5 individual **Policies**.

Global Policy is the system's universal policy and is applied to all clients unless the clients are bounded by another policy. Individual Policy can be defined and applied to different authentication server.

A client logging in with this authentication server will be bound by the corresponding Policy.

If no policy is applied to the authentication server, its users will be governed by the Global Policy.

Global Policy

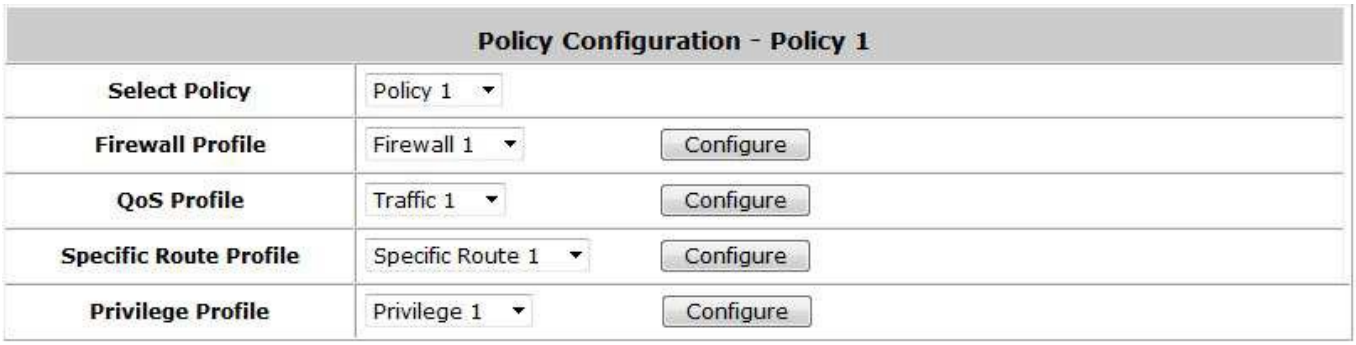
Global policy is the system's universal policy containing the **Firewall Profile**, **Specific Routes Profile (IPv4/IPv6)**, and **Privilege Profile**, which will be applied to all users unless the user has been regulated by another individual Policy.

Policy Configuration - Global Policy	
Select Policy	Global
Firewall Profile	Configure
Specific Route Profile	Configure
Specific IPv6 Route Profile	Configure
Privilege Profile	Configure

- **Select Policy:** Select a desired policy profile to configure.
- **Firewall Profile:** Global policy and policy 1 ~ 5 all have a firewall service list and a set of firewall profiles which is composed of firewall rules.
- **Specific Route Profile:** When Specific Routes are configured here, all clients applied with this policy will access the specific destination through these gateway settings.
- **Specific IPv6 Route Profile:** The routing rules to be applied to users using IPv6 under this policy may be configured here.
- **Privilege Profile:** Enable or Disable Users' privilege to change password. Administrator can set the maximum sessions per user here.

Policy 1 ~ Policy 5

Beside **Global Policy**, **Policy 1** to **Policy 5**, each consists of access control profiles that can be respectively configured and applied to a certain authentication server or user.



- **Select Policy:** Select a desired policy profile to configure.
- **Firewall Profile:** Each Policy has a firewall service list and a set of firewall profiles consisting of firewall rules.
- **QoS Profile:** QoS profile defines the traffic class for the users governed by this Policy.
- **Specific Route Profile:** The default gateway of a desired IP address can be defined in a policy. When Specific Routes are configured here, all clients applied with this policy will access the specific destination through these gateway settings.
- **Privilege Profile:** Enable or Disable Users' privilege to change password. Administrator can set the maximum sessions per user here.

6.3.1 Schedule

> **Schedule Profile:** Click ***User >> Schedule*** to enter the configuration page and shows the **Permitted Login Hours** list. This function is used to limit the time when clients can log in. Check the desired time-slot checkboxes and click ***Apply*** to save the settings. These settings will become effective immediately after clicking ***Apply***.

Administrator can also choose to **Enable** or **Disable** Auto logout when a user exceeds the permitted login hours.

Up to 5 profiles can be configured.

Schedule Configuration	
Auto logout station by system	○ Enable ◉ Disable

Apply Cancel

Permitted Login Hours - Profile 1							
Select Profile	Profile 1						
HOUR	**SUN**	**MON**	**TUE**	**WED**	**THU**	**FRI**	**SAT**
00:00~00:59	☑	☑	☑	☑	☑	☑	☑
01:00~01:59	☑	☑	☑	☑	☑	☑	☑
02:00~02:59	☑	☑	☑	☑	☑	☑	☑
03:00~03:59	☑	☑	☑	☑	☑	☑	☑
04:00~04:59	☑	☑	☑	☑	☑	☑	☑
05:00~05:59	☑	☑	☑	☑	☑	☑	☑
06:00~06:59	☑	☑	☑	☑	☑	☑	☑

6.3.2 Firewall

Firewall Profile: Click ***User >> Firewall*** and the Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules. Up to 5 profiles can be configured.

Firewall Configuration - Profile 1	
Select Profile	Profile 1
Predefined and Custom Service Protocols	Configure
User Firewall Rules	Configure
User Firewall Rules (IPv6)	Configure

1) Predefined and Custom Service Protocols

Predefined and Custom Service Protocols: There are predefined service protocols available for firewall rule editing.

Firewall Profile 1 - Service Protocols List			
No.	**Name**	**Description**	Select All
0	ALL	ALL	☐
1	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	☐
2	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	☐
3	ALL ICMP	ICMP; Type: Any, Code: Any	☐
4	FTP	TCP/UDP; Destination Port: 20;21	☐
5	HTTP	TCP/UDP; Destination Port: 80	☐
6	HTTPS	TCP/UDP; Destination Port: 443	☐
7	POP3	TCP; Destination Port: 110	☐
8	SMTP	TCP; Destination Port: 25	☐
9	DHCP	UDP; Destination Port: 67;68	☐
10	DNS	TCP/UDP; Destination Port: 53	☐

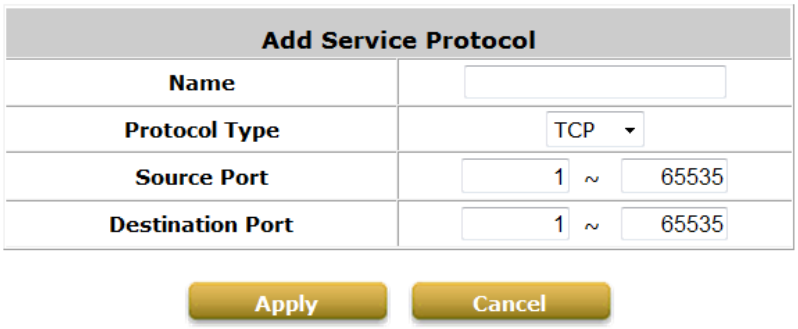
The administrator is able to add new custom service protocols by clicking ***Add***, and delete the added protocols individually or with ***Select All*** followed by ***Delete*** operation.

Caution:

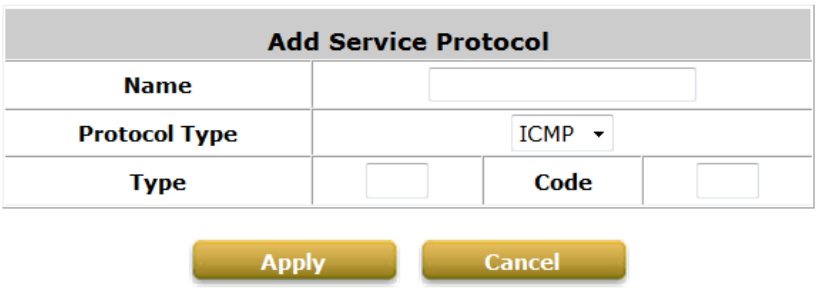
The Predefined Service Protocols cannot be deleted.

Click **Add** to add a custom service protocol.

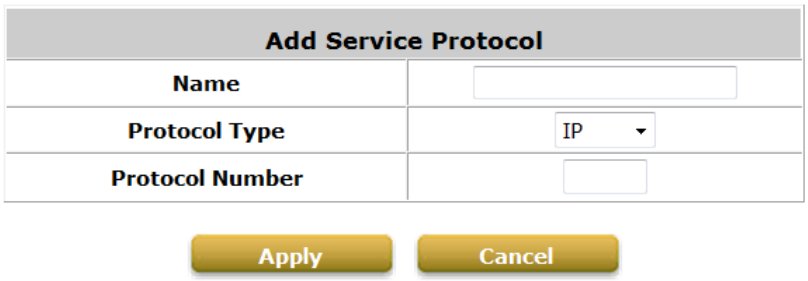
The **Protocol Type** can be defined from a list of service by protocols (*TCP/UDP/ICMP/IP*); and then define the **Source Port** (range) and **Destination Port** (range); click ***Apply*** to save this protocol.



If the **Protocol Type** is **ICMP**, the **Type** and **Code needs to be defined**.



If the **Protocol Type** is **IP**, the **Protocol Number needs to be defined**.



2) User Firewall Rules

After the custom protocol is defined(or just use the **Predefined Service Protocols)**, you will need to enable the **Firewall Rule** to apply these protocols. Firewall Rules for IPv6 is also supported.

- **Firewall Rules:** Click ***Rule No.*** to edit individual rules and click ***Apply*** to save the settings. The rule status will be shown on the list. Check the **"Active"** checkbox and click ***Apply*** to enable the rule. Rule No.1 has the highest priority; Rule No.2 has the second priority and so on. Each firewall rule is defined by Source, Destination and Pass/Block action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to **Always**, **Recurring** or **One Time**.

Selecting the Filter Rule Number 1 as an example:

Policy 1 - Edit Filter Rule			
Rule Number	1		
Rule Name			
Source		**Destination**	
Interface/Zone	ALL	**Interface/Zone**	ALL
IP Address	0.0.0.0	IP Address	0.0.0.0
Subnet Mask	0.0.0.0 (/0)	**Subnet Mask**	0.0.0.0 (/0)
MAC Address			
Service Protocol	ALL		
Schedule	Always Recurring One Time		
Action for Matched Packets	Block Pass		

- **Rule Number:** This is the rule selected "1". Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on.
- **Rule Name:** The rule name can be changed here.
- **Source/Destination – Interface/Zone:** There are choices of **ALL, WAN**, **Public** and **Private** to be applied for the traffic interface.
- **Source/Destination – IP Address/Domain Name:** Enter the source and destination IP addresses. Domain Name filtering is supported but Domain Host filtering is not.
- **Source/Destination – Subnet Mask:** Select the source and destination subnet masks.
- **Source- MAC Address:** The MAC Address of the source IP address. This is for specific MAC address filtering.
- **Service Protocol:** These are defined protocols on the **service protocols list** to be selected.
- **Schedule:** When schedule is selected, clients assigned with this policy are applied the firewall rule only within the time checked. There are three options, **Always**, **Recurring** and **One Time. Recurring** is set with the hours within a week.
- **Action for Matched Packets:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.

6.3.3 QoS Profile

Up to 5 QoS profiles can be configured for certain applications or users that need stable bandwidth or traffic priority.

Bandwidth Control can only be Enabled when Bandwidth limits on WAN has been Enabled.

Traffic Configuration - Profile 1	
Select Profile	Profile 1
Traffic Class	IPv4 IPv6
Bandwidth Control	Enable Disable
Group Total Downlink	0 Mbps *(Unlimit: 0, Range: 1-999)
Individual Maximum Downlink	0 Mbps *(Unlimit: 0, Range: 1-999)
Individual Request Downlink	0 Mbps *(Unlimit: 0, Range: 1-999)
Group Total Uplink	0 Mbps *(Unlimit: 0, Range: 1-999)
Individual Maximum Uplink	0 Mbps *(Unlimit: 0, Range: 1-999)
Individual Request Uplink	0 Mbps *(Unlimit: 0, Range: 1-999)

> **Traffic Class**: Traffic Class can be chosen for users on IPv4 or IPv6. Default DSCP (Differentiated Services Code Point) can be added and edited to determine traffic class. Default DSCP includes: Network Control 0x30, Telephony 0x2E, Signaling 0x28, Multi-media Conferencing 0x26, Real-Time Interactive 0x20, Multi-media Streaming 0x1A, Broadcast Video 0x18, Low-latency Data 0x12, OAM 0x10, High-Throughput Data 0x0A, Standard 0x00, Low Priority Data 0x08.

> **Bandwidth Control**: Enable or Disable the capability to determine the following parameters.

> **Group Total Downlink**: Defines the maximum bandwidth allowed to be shared by clients.

> **Individual Maximum Downlink**: Defines the maximum downlink bandwidth allowed for an individual client. The Individual Maximum Downlink cannot exceed the value of Group Total Downlink.

> **Individual Request Downlink:** Defines the guaranteed minimum downlink bandwidth allowed for an individual client. The Individual Request Downlink cannot exceed the value of Group Total Downlink and Individual Maximum Downlink.

> **Group Total Uplink:** Defines the maximum uplink bandwidth allowed to be shared by clients.

> **Individual Maximum Uplink:** Defines the maximum uplink bandwidth allowed for an individual client. The Individual Maximum Uplink cannot exceed the value of Group Total Uplink.

> **Individual Request Uplink:** Defines the guaranteed minimum bandwidth allowed for an individual client. The Individual Request Uplink cannot exceed the value of Group Total Uplink and Individual Maximum Uplink.

6.3.4 Routing

Specific Route Profile: Click ***User >> Specific Route*** for the **Specific Route Profile**, the 'Specific Route Profile' list will appear.

1) Specific Route

Specific Route Profile: The Specific Default Route is used to control clients to access some specific IP segment by the specified gateway. Specific Routing can be set up for the Global Policy and up to 5 profiles can be configured.

Global Policy - Specific Routes

Route No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1		255.255.255.255 (/32)	
2		255.255.255.255 (/32)	
3		255.255.255.255 (/32)	
4		255.255.255.255 (/32)	

Specific Routes - Profile 1

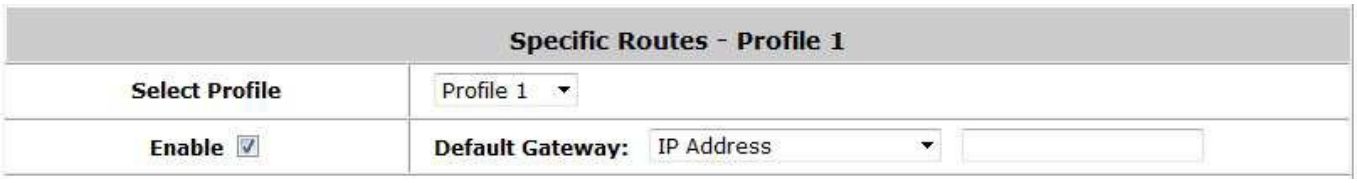
Select Profile	Profile 1
Enable ☐	Default Gateway: IP Address

Route No.	Destination		Gateway
	IP Address	Subnet Netmask	IP Address
1		255.255.255.255 (/32)	
2		255.255.255.255 (/32)	
3		255.255.255.255 (/32)	
4		255.255.255.255 (/32)	
5		255.255.255.255 (/32)	
6		255.255.255.255 (/32)	
7		255.255.255.255 (/32)	
8		255.255.255.255 (/32)	

- **Destination / IP Address:** The destination network address or IP address of the destination host. Please note that, if applicable, the system will calculate and display the appropriate value based on the combination of Network/IP Address and Subnet Mask that have just been entered and applied.
- **Destination / Subnet Netmask:** The subnet mask of the destination network. Select *255.255.255.255(/32)* if the destination is a single host.
- **Gateway / IP Address:** The IP address of the gateway or next router to the destination.

2) Default Gateway

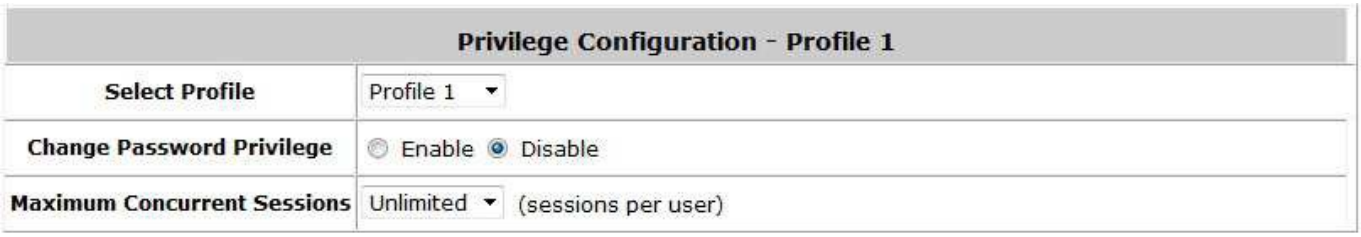
Default Gateway: The default gateway of a desired IP address can be defined in each Policy except Global Policy. When Specific Default Route is enabled, all clients applied with this Policy will access the Internet through this default gateway.



- **Enable:** Check ***Enable*** box to activate this function or uncheck to deactivate it.
- **Default Gateway IP Address**: You may need to fill in the IP address of the default gateway.

6.3.5 User Privilege

Administrator can choose to allow users to change their Password. And to prevent ill-behaved clients or malicious software from taking up the system's connection resources, the administrator can restrict the number of concurrent sessions that a user can establish.



> The maximum number of concurrent sessions including TCP and UDP for each user can be specified in the Global policy, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones.
Also, this can be specified in the other policies to apply to the authenticated users.

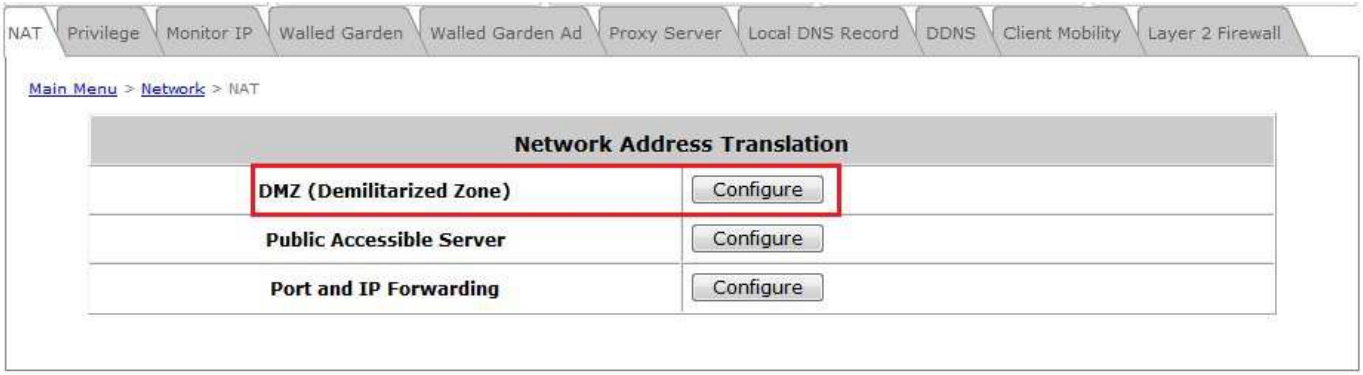
> When the number of a user's sessions reach the session limit (a choice of Unlimited, 10, 25, 50, 100, 200, 350, 500, 750 and 1000), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to a SYSLOG server.

Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in network deployment to maintain network operation.

7 Access Network without Authentication

7.1 DMZ

To configure DMZ, go to: ***Network >> Network Address Translation >> DMZ (Demilitarized Zone)***.



There are 40 sets of static Internal IP Address and External IP Address available.

Enter **Internal** and **External** IP Address as a set. After the setup, accessing the External IP address listed in DMZ will be mapped to accessing the corresponding Internal IP Address.

These settings will become effective immediately after clicking the ***Apply*** button.

The External IP Address of the Automatic WAN IP Assignment is the IP address of External Interface (WAN) that will change dynamically if WAN Interface is Dynamic.

When **Automatic WAN IP Assignments** is enabled, the entered Internal IP Address of Automatic WAN IP Assignment will be bound with WAN interface.

Automatic WAN IP Assignment

Enable	External IP Address	External Interface	Internal IP Address	Remark
☐	10.16.29.79	WAN		

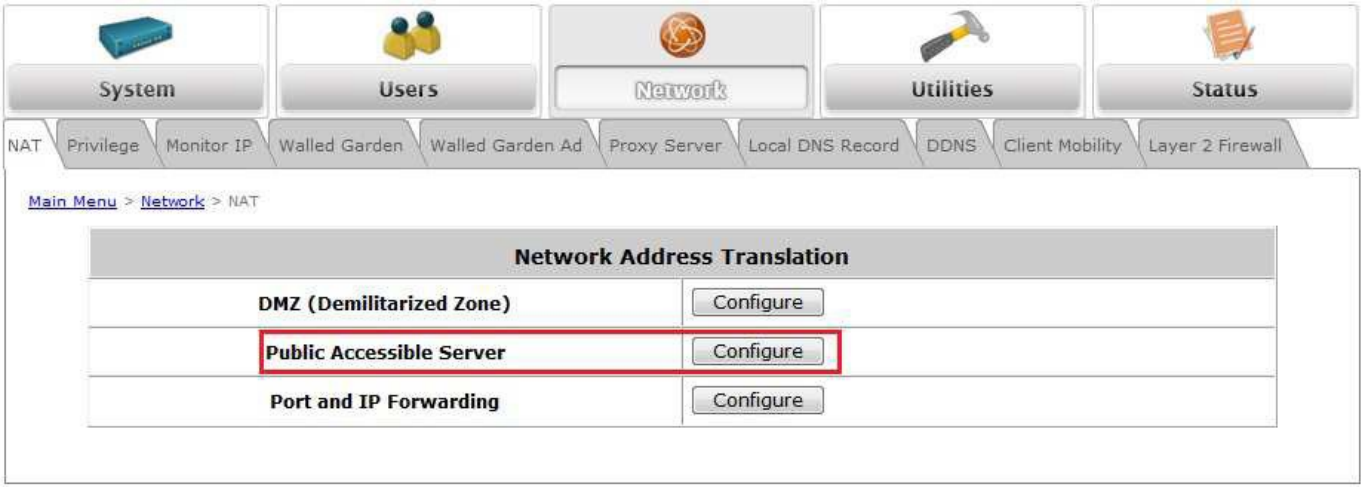
Static Assignments

No.	External IP Address	External Interface	Internal IP Address	Remark
1		WAN		
2		WAN		
3		WAN		
4		WAN		
5		WAN		
6		WAN		
7		WAN		
8		WAN		
9		WAN		
10		WAN		

(Total:40) First Prev Next Last Go to Page 1 (Page:1/4) Row per Page: 10

7.2 Virtual Server

To configure Virtual Server, go to: ***Network >> Network Address Translation >> Public Accessible Server***.



This function allows the administrator to set 40 virtual servers at most, so that client devices outside the managed network can access these servers within the managed network.

Different virtual servers can be configured for different sets of physical services, such as TCP and UDP services in general.

Enter the **"External Service Port"**, **"Local Server IP Address"** and **"Local Server Port"**. Select **"TCP"** or **"UDP"** for the service type.

In the **Enable** column, check the desired server to enable.

These settings will become effective immediately after clicking the ***Apply*** button.

Public Accessible Server

No.	External Service Port	Local Server IP Address	Local Server Port	Type	Enable	Remark
1				TCP / UDP		
2				TCP / UDP		
3				TCP / UDP		
4				TCP / UDP		
5				TCP / UDP		
6				TCP / UDP		
7				TCP / UDP		
8				TCP / UDP		
9				TCP / UDP		
10				TCP / UDP		

7.3 Privilege List

To configure the Privilege List, go to: ***Network >> Privilege***

Setup the **Privilege IP Address List**, **Privilege MAC Address List** and the **Privilege IPv6 Address List**.

The clients accessing the internet via IP addresses and/or networking devices on the list can access the network without any authentication.

7.3.1 Privilege IP

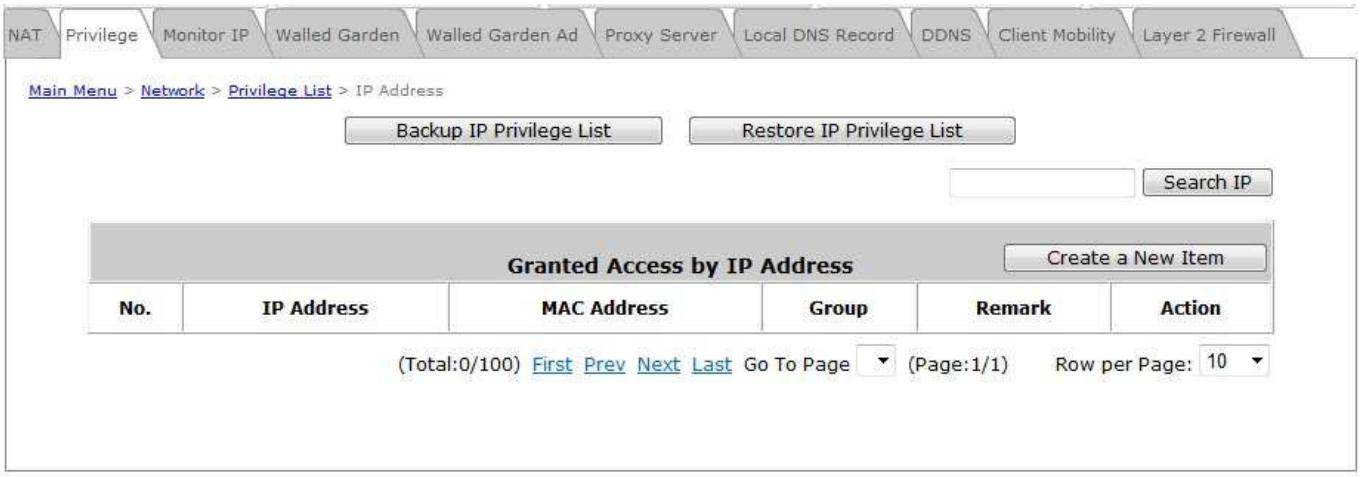
Privilege IP Address List

To configure Privilege IP Address List, go to: ***Network >> Privilege >> IP Address List***.

If there are workstations inside the managed network that need to access the network without authentication, enter the IP addresses of these workstations in **"Granted Access by IP Address"**.

The **"Remark"** field is not necessary but is convenient for keeping track. The RAYTALK RA-696 allows 100 privilege IP addresses at most.

These settings will become effective immediately after clicking ***Apply***.



Caution:

Permitting specific IP addresses to have network access rights without going through standard authentication process under Public zone may cause security problems.

7.3.2 Privilege MAC

Privilege MAC Address List

In addition to the Privilege IP List, MAC address List allows the MAC address of the workstations that need to access the network without authentication to be set in **"Granted Access by MAC Address"**.

The RAYTALK RA-696 allows 100 privilege MAC addresses at most.

When manually creating the list, enter the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as the remark (optional).

These settings will be effective immediately after clicking ***Apply***.

Granted Access by MAC Address		
No.	**MAC Address**	**Remark**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(Total: 100) First Prev Next Last

Caution:

Permitting specific MAC addresses to have network access rights without going through standard authentication process under Public zone may cause security problems.

7.3.3 Privilege IPv6

Privilege IPv6 Address List

In addition to the Privilege IP List, MAC address List, the privilege IPv6 List allows the IPv6 address of the workstations that need to access the network without authentication to be set in **"Granted Access by IPv6 Address"**. The RAYTALK RA-696 allows 100 privilege IPv6 addresses at most.

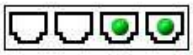
When manually creating the list, enter the IPv6 address (the format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx) as well as the remark (optional).

These settings will be effective immediately after clicking ***Apply***.

7.4 Disable Authentication in Public Zone

To disable Authentication in Public Zone, go to: ***System >> Service Zones,*** *click* ***Configure*** *in* ***Public Zone***.

Service Zone Settings

Service Zone Name	Applied Policy / Default Authen Option	IP Address / IPv6 Address	Network Alias	DHCP Pool	LAN Port Mapping / Status	Details
Private	Policy 1	192.168.1.254	N/A	192.168.1.1 ~ 192.168.1.100		Configure
	Disabled	N/A			Enabled	
Public	Policy 1	172.21.0.254	N/A	172.21.0.1 ~ 172.21.0.100		Configure
	Server 1	N/A			Enabled	

Authentication Settings

Authentication Required For the Zone	(•) Enable ( ) Disable ( ) Suspend				
WISPr Configuration	Configure				
Authentication Options	**Auth Option**	**Auth Database**	**Postfix**	**Default**	**Enable**
	Server 1	LOCAL	local	(•)	☑
	Server 2	RADIUS	radius1	( )	☑
	Server 3	RADIUS	radius2	( )	☑
	On-demand User	ONDEMAND	ondemand	( )	☑
	FREE	FREE	N/A	( )	☐

Authentication Required For the Zone: When it is disabled, users will not need to authenticate before they get access to the network within Public Zone.

8 User Login and Logout

8.1 Before Login

8.1.1 Login with SSL

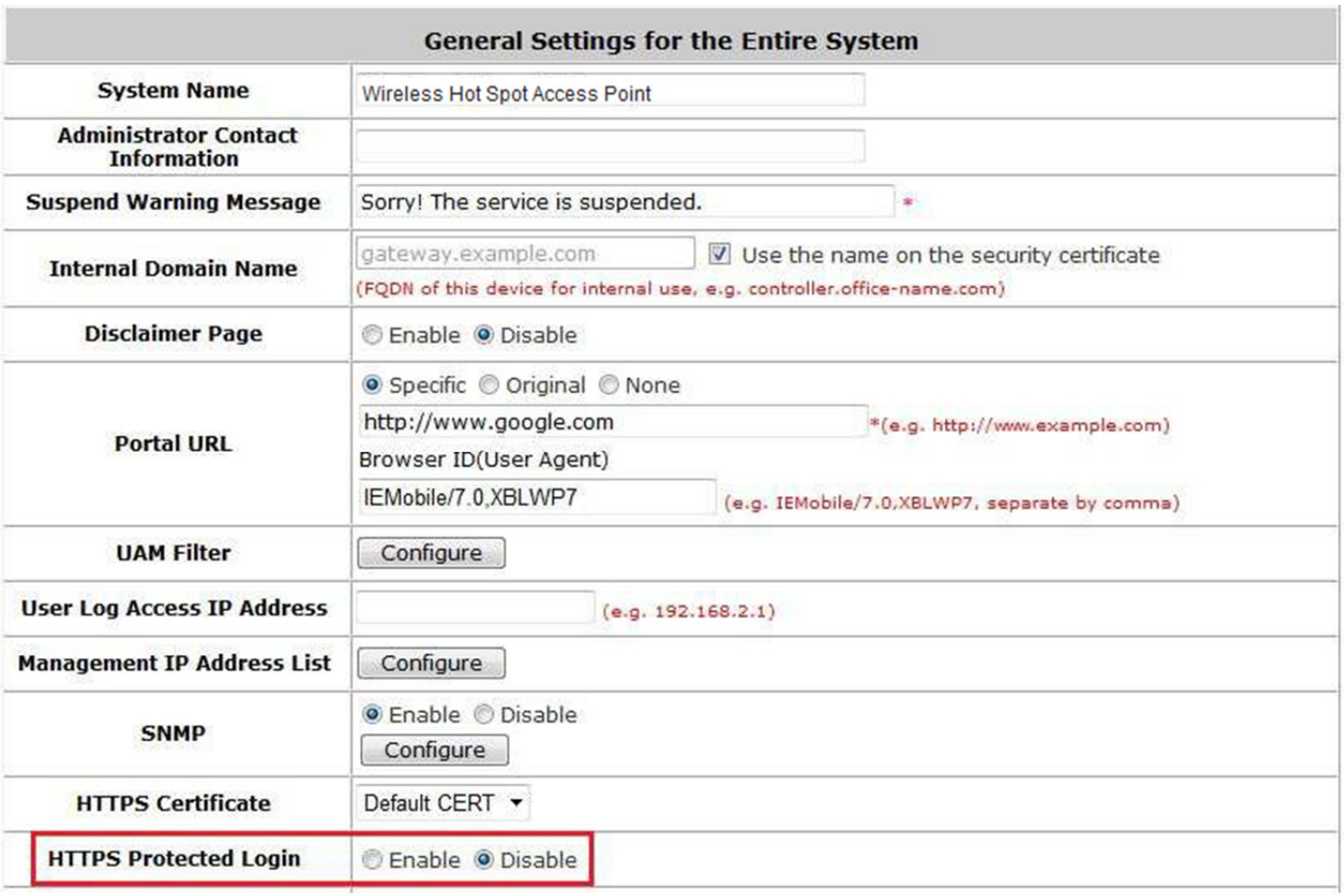
To configure HTTPS, go to: ***System >> General***.

HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering.

HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

The **HTTPS Protected Login** function makes the client's login more secure.

Enable it to activate https (encryption) or disable it to activate http (non encryption) login page.



8.1.2 Internal Domain Name with Certificate

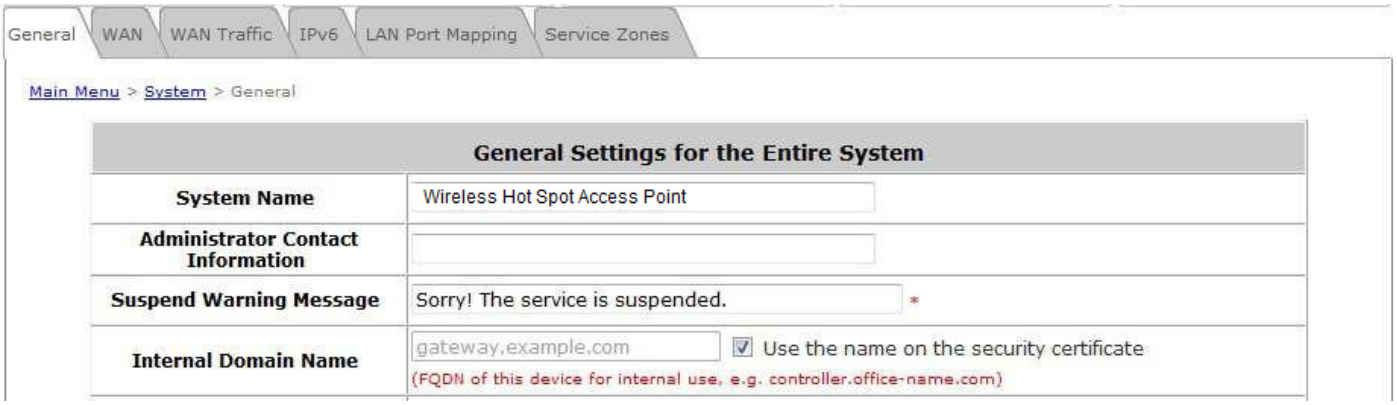
To configure Internal Domain Name, go to: ***System >> General***.

Internal Domain Name is the domain name of the RAYTALK RA-696 seen on client machines connected under zone.

It must conform to FQDN (Fully-Qualified Domain Name) standard.

A user on client machine can use this domain name to access the RAYTALK RA-696 instead of its IP address.

In addition, when "***Use the name on the security certificate***" option is checked, the system will use the CN (Common Name) value of the uploaded SSL certificate as the domain name.



To Configure Certificate, go to: ***Utilities >> Certificate*** and choose Upload Certificate from the scroll down menu.

Certificate: A data record used for authenticating network entities such as a server or a client.

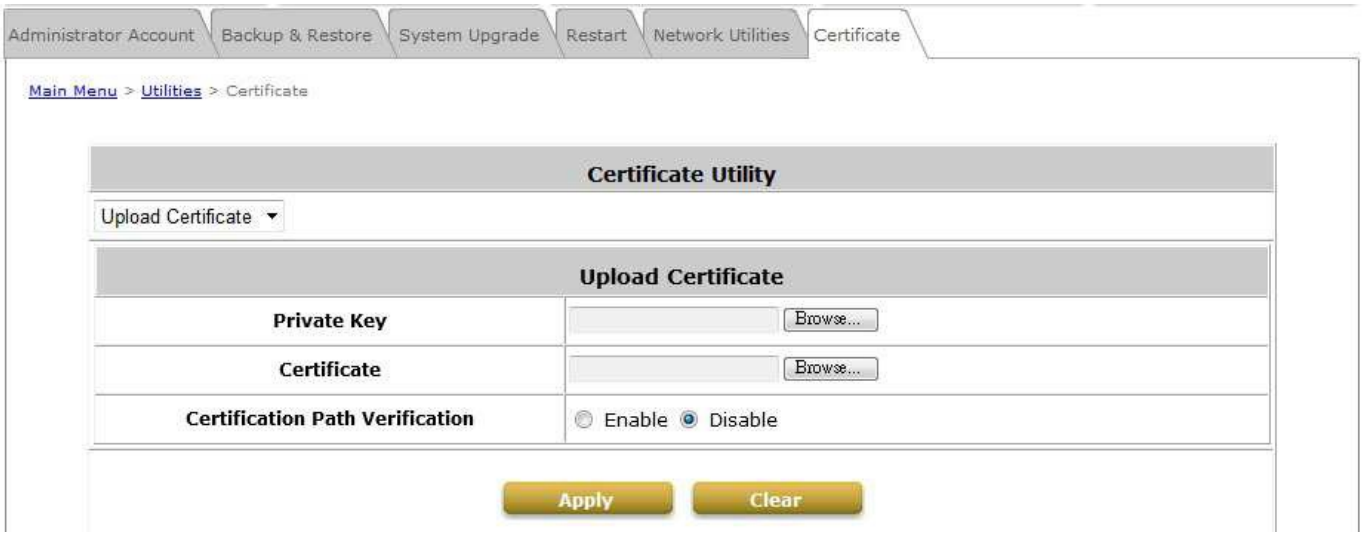
A certificate contains X.509 information pieces about its owner (called the subject) and the signing Certificate Authority (called the issuer), plus the owner's public key and the signature made by the CA.

Network entities verify these signatures using CA certificates.

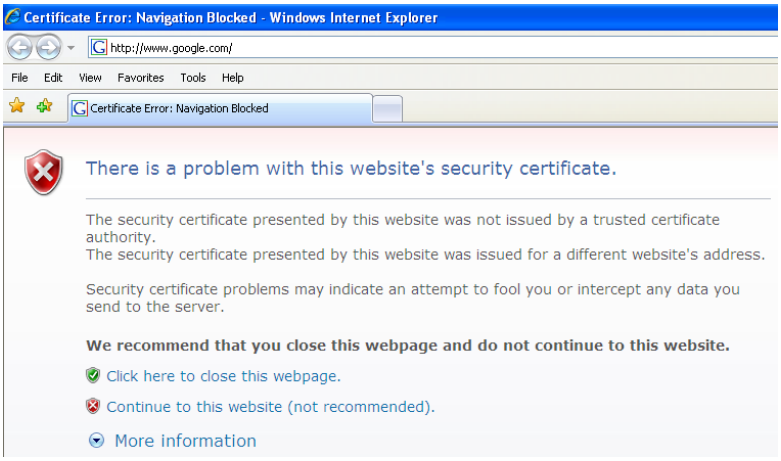
You can apply for a SSL certificate at CAs such as VeriSign.

If you already have a SSL Certificate, please Click **Browse** to select the file and upload it.

Click ***Apply*** to complete the upload process. If you do not have a valid SSL Certificate, use the system default certificate.



Without a valid certificate, users may encounter the following warning when trying to open the login page.


Certificate Error: Navigation Blocked - Windows Internet Explorer
http://www.google.com/
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Click "Continue to this website" to access the user login page.

8.1.3 Walled Garden

To configure Walled Garden, go to: ***Network >> Walled Garden***.

This function provides certain free services for users to access the websites listed here before login and authentication.

Up to 20 addresses or domain names of the websites can be defined on this list.

Users without the network access right can still have a chance to experience the actual network service free of charge.

Enter the **IP Address** or **Domain Name** (of the website) on the list and click ***Apply*** to save the settings.

Add Walled Garden List				
No.	Active	Domain Name/IP Address	Service Zone	Remark
1	☐		All	
2	☐		All	
3	☐		All	
4	☐		All	
5	☐		All	
6	☐		All	
7	☐		All	
8	☐		All	
9	☐		All	
10	☐		All	

8.1.4 Walled Garden AD

To configure Walled Garden AD List, go to: ***Network >> Walled Garden AD***.

This function provides advertisement links to web pages for users to access free of charge before login and authentication. Advertisement hyperlinks are displayed on the user's login page.

Clients who click on it will be redirected to the listed advertisement websites.

Walled Garden Ad List				
Item	URL	Topic	Edit	Display
	Description			
1			Edit	
2			Edit	
3			Edit	
4			Edit	
5			Edit	
6			Edit	
7			Edit	
8			Edit	
9			Edit	
10			Edit	

Enter all items or make changes by clicking the ***Edit*** button, click ***Apply***, the items will be added and shown on the list.

- **URL:** Enter the URL of the advertisement website.
- **Topic:** Enter the content of the hyperlink, for instance if you enter Google in this field, on the user login page a hyperlink of Google will be displayed.
- **Description:** Any additional message for administrator's reference.
- **Display:** Choose ***Display*** to display advertisement hyperlinks on the login pages.

8.2 After Login

8.2.1 Portal URL after successful login

To configure Portal URL after a successful user login, go to: ***System >> General***.

When this function is enabled, enter the URL of a Web server as the Portal page.

Once logged in successfully, users will be directed to this URL, such as *http://www.google.com*, regardless of the original homepage set in their browsers.

When this function is set to ***None***, after users logged in successfully, users will be directed to the original homepage set in their browsers.

8.2.2 Idle Timer

To configure Idle Timer, go to: ***Users >> Additional Control***.

If a user has idled with no network activities, the system will automatically kick the user out.

The logout timer can be set between 1~1440 minutes, and the default idle time is 10 minutes.

Additional Control		
User Session Control	Idle Timeout (minutes)	10 *(1-1440)
	Interval for Idle Traffic Detection (seconds)	60 *(1-600)
	Threshold for Idle Traffic Detection (bytes)	0 *(0-1048576, 0 is Disabled)
	Idle Timeout Check Direction	○ Uplink ◉ Uplink & Downlink
	Multiple Login	☐ Enable (This function is not applicable to on-demand accounts.)
	Charge Traffic to/from Hosts in Walled Garden List	○ Enable ◉ Disable
	Kick out users when their IPs are changed	○ Enable ◉ Disable

8.2.3 Multiple Login

To configure Multiple Login, go to: ***Users >> Additional Control***.

When enabled, a user can log in from different computers with the same account (this function doesn't support On-demand users.)

Additional Control		
User Session Control	Idle Timeout (minutes)	10 *(1-1440)
	Interval for Idle Traffic Detection (seconds)	60 *(1-600)
	Threshold for Idle Traffic Detection (bytes)	0 *(0-1048576, 0 is Disabled)
	Idle Timeout Check Direction	○ Uplink ◉ Uplink & Downlink
	Multiple Login	☐ Enable (This function is not applicable to on-demand accounts.)
	Charge Traffic to/from Hosts in Walled Garden List	○ Enable ◉ Disable
	Kick out users when their IPs are changed	○ Enable ◉ Disable

9 Networking Features of a Gateway

9.1 IP Plug and Play

To configure IP Plug and Play, go to: ***Network >> Client Mobility***.

The RAYTALK RA-696 supports IP PNP function.

A user can log in and access network with any IP address setting.

This function is disabled in default settings.

Client Mobility	
IP PNP	○ Enable ◉ Disable

When **IP PNP** is enabled, at the user end, a static IP address can be used to connect to the system.

Regardless of what the IP address at the user end is using, authentication can still be performed through the RAYTALK RA-696.

9.2 Dynamic Domain Name Service (DDNS)

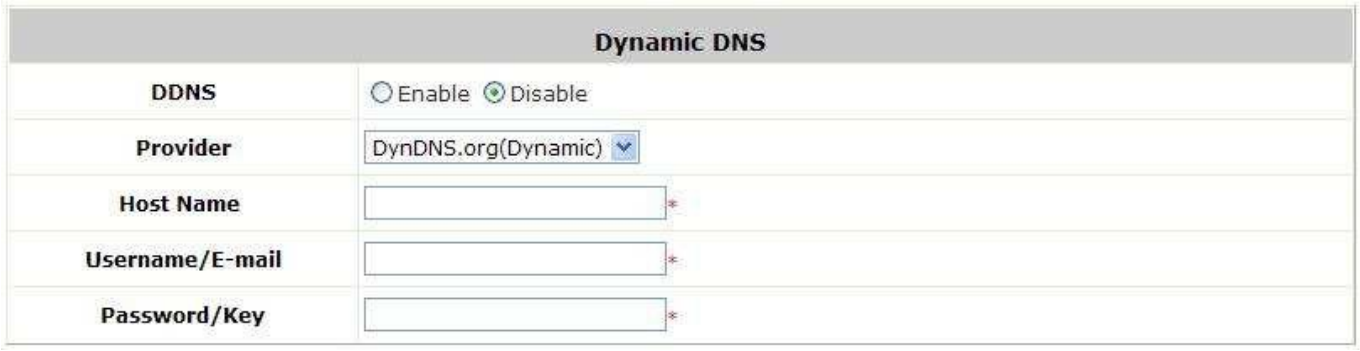
To configure Dynamic Domain Name Service, go to: ***Network >> DDNS***.

Before activating this function, you must have your Dynamic DNS hostname registered with a Dynamic DNS provider.

The MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696 supports DNS function to alias the dynamic IP address for the WAN port to a static domain name, allowing the administrator to easily access the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696's WAN.

If the dynamic DHCP is activated at the WAN port, it will update the IP address of the DNS server periodically.

These settings will become effective immediately after clicking ***Apply***.



- **DDNS:** Enable or disable this function.
- **Provider:** Select the DNS provider.
- **Host name:** The IP address/domain name of the WAN port.
- **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- **Password/Key:** The register password for the DNS provider.

Note:

To apply for free Dynamic DNS service, you may go to http://www.dyndns.com/services/dns/dyndns/howto.html.

9.3 Port and IP Forwarding

To configure Port and IP Forwarding, go to: ***Network >> NAT >> Port and IP Forwarding***.

This function allows the administrator to set at most 40 sets of IP addresses for redirection purposes.

When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination.

Please enter the **"IP Address"** and **"Port"** of **Destination**, and the **"IP Address"** and **"Port"** of **Translated to Destination**. Select **"TCP"** or **"UDP"** for the service's type.

These settings will become effective immediately after clicking ***Apply***.

Port and IP Forwarding

No.	Destination		Translated to Destination		Type	Remark
	IP Address	Port	IP Address	Port		
1					TCP / UDP	
2					TCP / UDP	
3					TCP / UDP	
4					TCP / UDP	
5					TCP / UDP	
6					TCP / UDP	
7					TCP / UDP	
8					TCP / UDP	
9					TCP / UDP	
10					TCP / UDP	

10 System Management and Utilities

10.1 System Time

To configure System Time, go to: ***System >> General***.

NTP (Network Time Protocol) communication protocol can be used to synchronize the system time with remote time server. Please specify the local time zone and the IP address of at least one NTP server for adjusting the time automatically (Universal Time is Greenwich Mean Time, GMT).

Manual setup is another option to set up the system time, if you choose to set up the system time manually, please enter the Year, Month, Day, the current time and click Apply to activate the changes.

NTP Server Mode: When Enabled, Access Points and devices in the Local Area Network of the gateway would be able to use the gateway as a NTP Server for time reference.

Note:

When system cannot sync the time with NTP server, all clients will not be allowed to log in to system. Also on-demand accounts cannot be created.

10.2 Management IP Address List

To configure the Management IP Address List, go to: ***System >> General***.

Only PCs within the Management IP range on the list are allowed to access the system's web management interface.

Management IP Address List					
No.	Active	IP Address/Segment	No.	Active	IP Address/Segment
1	☑	0.0.0.0/0.0.0.0	2	☐	
3	☐		4	☐	
5	☐		6	☐	
7	☐		8	☐	
9	☐		10	☐	
11	☐		12	☐	
13	☐		14	☐	
15	☐		16	☐	
17	☐		18	☐	
19	☐		20	☐	

The default value is “0.0.0.0/0.0.0.0”. It means that the WMI can be accessed by any IP address, for security consideration; please change this value before the system provides service.

10.3 IP Address for Accessing User Log

To configure User Log Access IP History, go to: ***System >> General***.

Specify an IP address of the administrator’s computer or a billing system to get billing history information of the RAYTALK RA-696 with the predefined URLs. The file name format is “yyyy-mm-dd”.

10.4 SNMP

To configure SNMP, go to: *System>> General.* The RAYTALK RA-696 supports SNMP v1/v2c.

If this function is enabled, the SNMP Management IP and the Community string can be assigned for SNMP management applications to access the system.

SNMP Configuration List			
Item	**Manager IP Address**	**Read Community**	**Write Community**
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

10.5 Administration

The RAYTALK RA-696 supports customizable administration account types, namely **Super Group**, **Manager, On-Demand Manager** or **Operator**.

The default predetermined group of the Administrator is Super group, and the username and password are as follows:

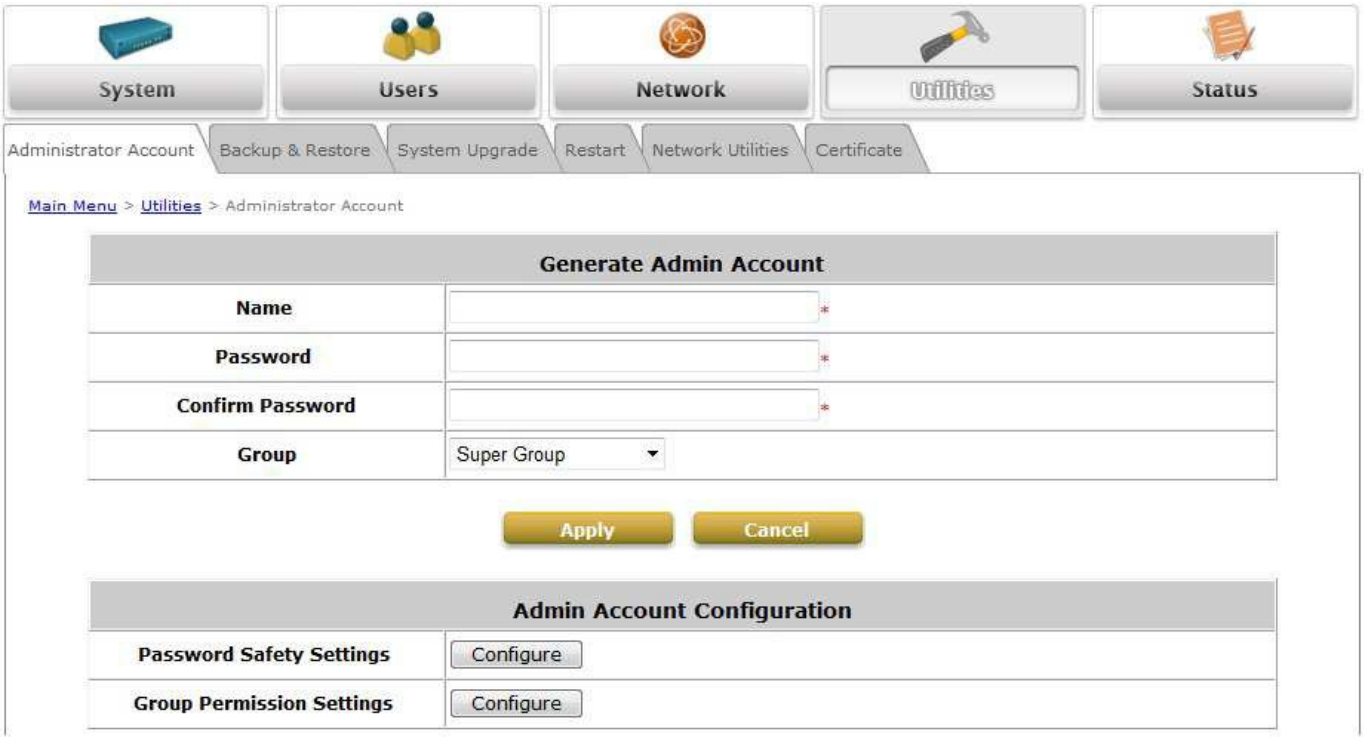
Admin: The administrator can access all configuration pages of the RAYTALK RA-696.

Username: **admin**

Password: **admin**

After a successful login to the RAYTALK RA-696, a web management interface with a Home manual will appear.

Admin is classified under Super Group, with all access and configuration authorities. Super Group members can generate other administrative accounts (Manager, OnDemand Manager and Operator) and configure Password Safety and Group Permission Settings.



Password Safety Settings:

Password rules and requirements can be configured here to facilitate additional security. The following parameters can be configured: **Password Complexity**, **Admin Login Retry Times**, **Password Expire**, and **Admin Login Reuse Times**.

There are three other default Administrative Account groups with predetermined permission settings, and these permission settings can be customized.

Manager: The manager can only access the configuration pages under **User Authentication** to manage the user accounts.

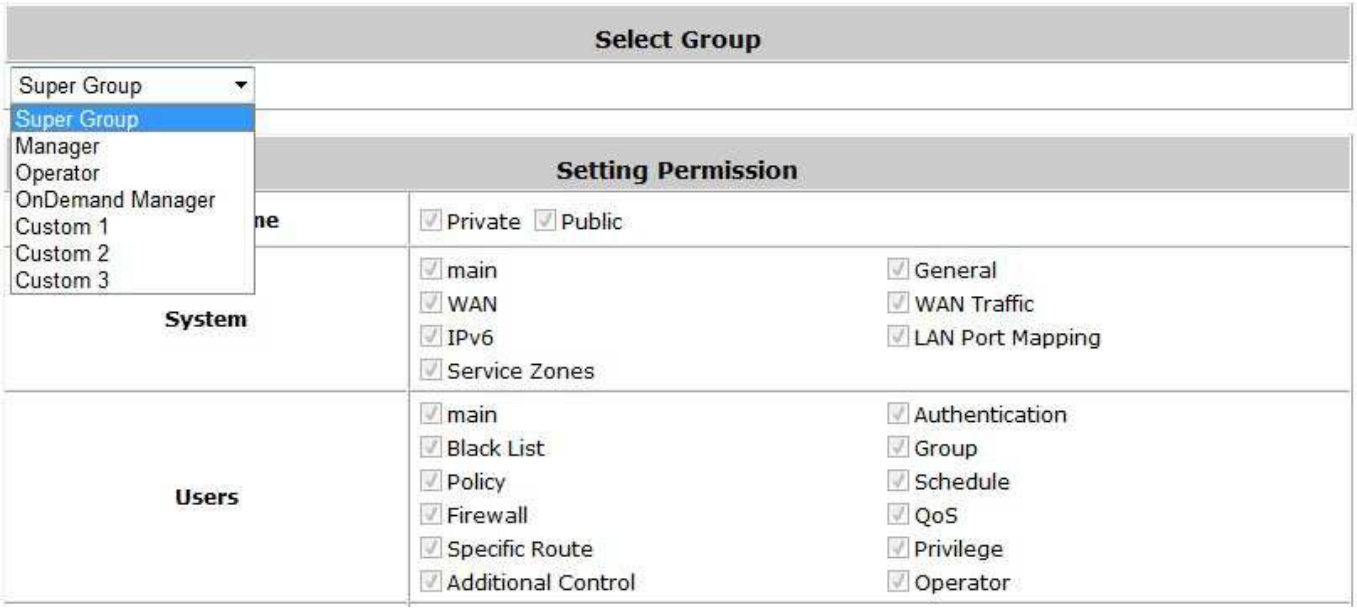
Operator: The operator can only access the configuration page of **Create On-demand User** to create new on-demand user accounts and print out the on-demand user account receipts.

On-demand Account Creation

Plan	Type	Quota	Price	Status	Function
1	Usage-time	15 min(s) connection time quota with expiration	10.91	Enabled	Create
2	Usage-time	11 min(s) connection time quota	1	Enabled	Create
3	Cut-off	Valid until 12:00 the following day	5	Enabled	Create
4	Duration-time	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1	Enabled	Create

OnDemand Manager: The OnDemand Manager can only access the **application programming interface** and generate on-demand user accounts from the API.

There are three additional custom groups for administrators to customize permission settings.



Note:

To logout, simply click the ***Logout*** icon on the upper right corner of the interface to return to the login screen.

10.6 Change Admin Passwords

To configure Admin passwords, go to: ***Utilities >> Administrator Account***.

There are four predetermined levels of authority: **Super Group**, **Manager**, **Operator**, and **On-Demand Manager**.

The usernames and passwords can be configured at: **Utilities >> Administrator Account**.

Clicking on the hyperlink of the Name allows the administrator to change passwords.

The administrator can change the passwords here.

Click Admin name on the Admin List, Enter original and new password and click ***Apply*** to activate the new password.

Note:
Only **admin** has the authority to change password.

Caution:
If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface via the serial console port.

10.7 Backup / Restore and Reset to the Factory Default

To configure Backup / Restore and Reset to Factory Default, go to: ***Utilities >> Backup & Restore***.

This function is used to backup/restore the RAYTALK RA-696 settings.

Also, the RAYTALK RA-696 can be restored to the factory default settings here.

- **Backup System Settings:** Click ***Backup*** to create a .db database backup file and save it on disk.
- **Restore System Settings:** Click ***Browse*** to search for a .db database backup file created by the RAYTALK RA-696 and click ***Restore*** to restore to the same settings at the time when the backup file was saved.
- **Reset to Factory Default:** Click ***Reset*** to load the factory default settings of the RAYTALK RA-696.

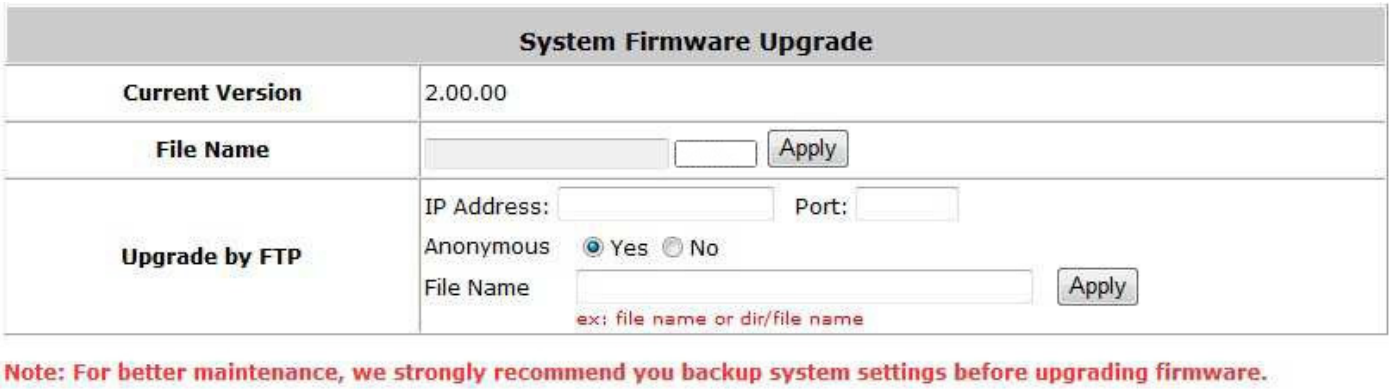
10.8 Firmware Upgrade

To configure Firmware Upgrade, go to: ***Utilities*** >> ***System Upgrade***.

The administrator can download the latest firmware from the website and upgrade the system here.

Select the latest firmware with ***Browse*** button, then click ***Apply***, the system will upload the file and restart to perform the upgrade process.

The firmware upgrade process can also be done via FTP. It might take a few minutes before the upgrade process completes and the new firmware's WMI interface appears.



Note:

*After clicking **Apply**, the system will begin uploading the chosen firmware into the system. Once the upload process is complete, the system will restart to activate the new firmware. The entire process may take a few minutes until the new firmware WMI appears. When restart is complete, system will not lease IP. So, please use static IP PC to upgrade system firmware.*

Caution:

1. Firmware upgrade may cause the loss of some data. You may need to manually backup user account information, please refer to the release notes for the limitation before upgrading.

2. Do not power on/off the system during the upgrade or restart process. It may damage the system and cause malfunction.

10.9 Restart

To perform system restart, go to: ***Utilities >> Restart***.

This function allows the administrator to safely restart the RAYTALK RA-696, and the process takes approximately three minutes.

Reason for restarting the system can be entered for record purposes.

Click ***YES*** to restart the RAYTALK RA-696; click ***NO*** to go back to the previous screen.

Do NOT power off during system restart as this might damage the system. If the

power needs to be turned off, it is highly recommended to restart the RAYTALK RA-696 first and then turn off the power after completing the restart process.

Caution:

The connection of all online users to the system will be disconnected when system is in the process of restarting.

10.10 Network Utility

To configure Network Utility, go to: ***Utilities >> Network Utilities***.

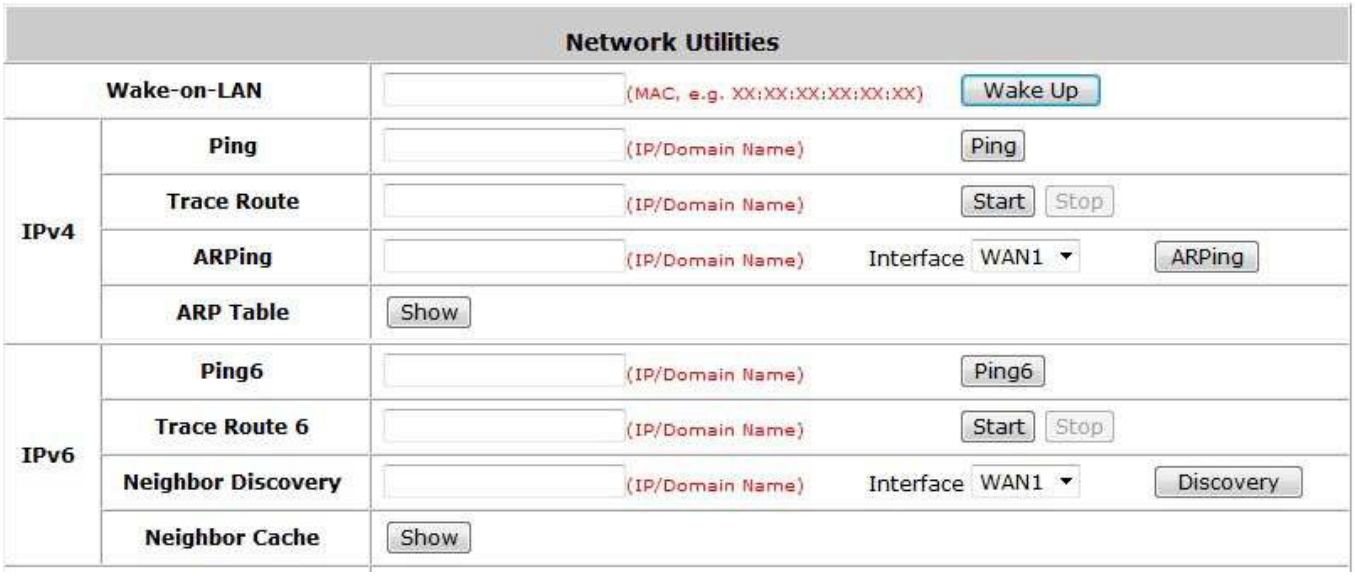
System provides some network utilities for administrators. Both IPv4 and IPv6 are supported.

Wake-on-LAN is for waking up remote devices that supports Wake-on-LAN feature by entering the MAC address of the target device and then press ***Wake Up*** button.

Ping is to see whether a destination host is reachable and alive by entering the destination host's domain name or IP address and then press ***Ping*** button.

Trace Route displays the actual route taken to reach the destination host. Entering the destination host's domain name or IP address and then press ***Start*** button to see the route.

ARP Table is for displaying ARP information stored on the system.



10.10.1 Wake-on-LAN

This allows the system to remotely boot up a power-down computer connected to a LAN port with Wake-On-LAN feature enabled in its BIOS. Enter the MAC Address of the desired device and click ***Wake Up*** to execute this function.

10.10.2 Ping

It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.

10.10.3 Trace Route

It allows administrator to find out the real path of packets from the gateway to a destination using IP address or Host domain name.

10.10.4 Show ARP Table

It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).

10.11 Monitor IP Link

To configure Monitor IP Link, go to: ***Network*** >> ***Monitor IP***.

The RAYTALK RA-696 will send out a packet periodically to monitor the connection status of the IP addresses on the list.

On each monitored item with a WEB server running, administrators may add a link for easy access by entering the IP, selecting the **Protocol** to *http* or *https* and then clicking ***Create***.

After clicking ***Create***, the IP address will become a hyperlink, and administrators can easily access the host remotely by clicking the hyperlink.

Click the ***Delete*** button to remove the hyperlink if needed.

Monitor IP List

No.	Protocol	IP Address	Hyperlink	Remark
1	http		Create	
2	http		Create	
3	http		Create	
4	http		Create	
5	http		Create	
6	http		Create	
7	http		Create	
8	http		Create	
9	http		Create	
10	http		Create	

10.12 Console Interface

Via the console port, administrators can enter the console interface to handle problems and situations occurred during operation.

1. In order to connect to the console port of the RAYTALK RA-696, a console, modem cable, and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **9600, 8, None, 1, None.**

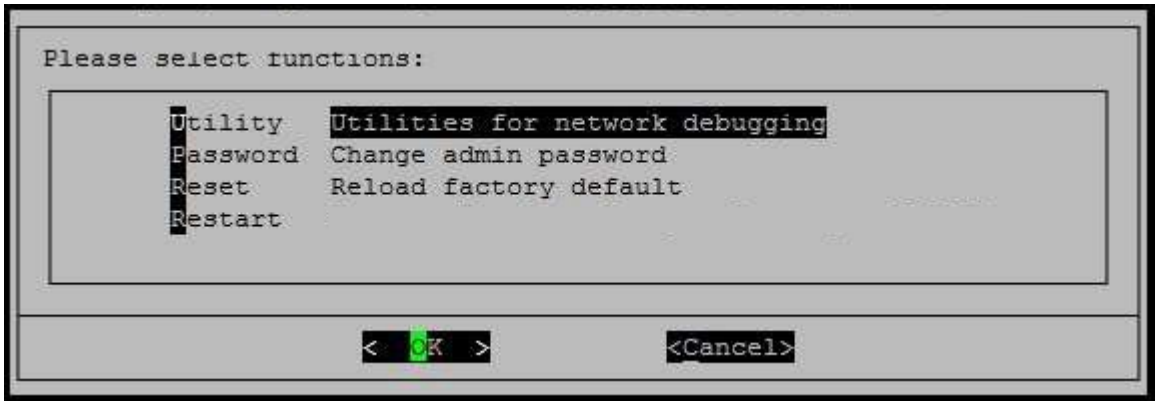
Caution:

*The main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the **Enter** key to make selection or confirm what you enter.*

3. Once the console port of the RAYTALK RA-696 is connected properly, the console main screen will appear automatically.

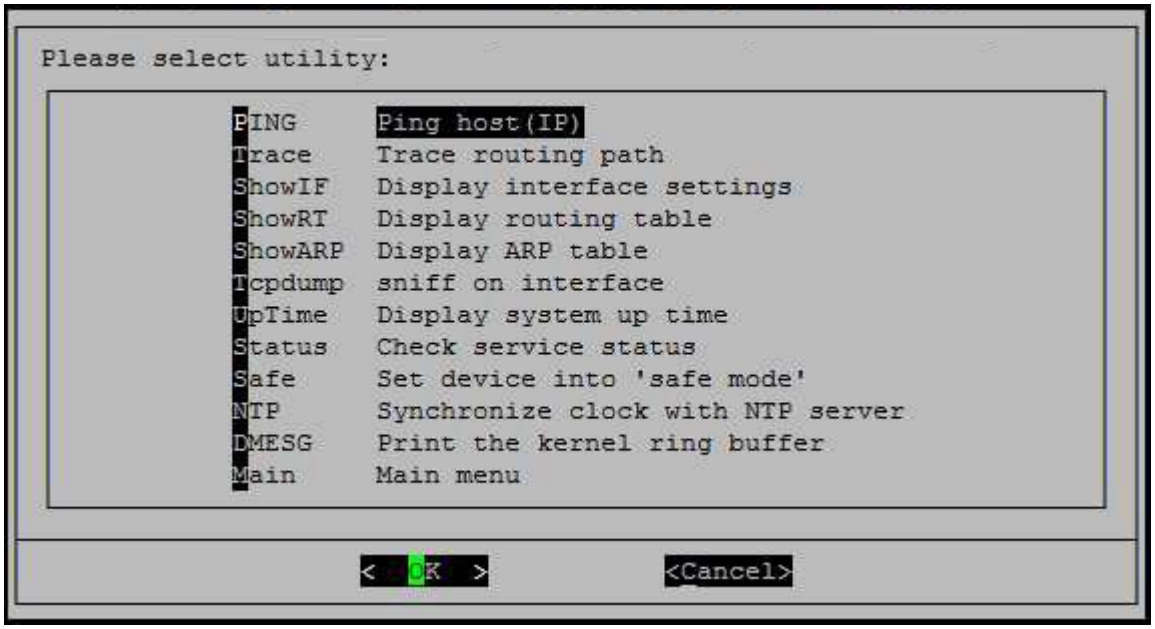
If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys so that the terminal simulation program will send some messages to the system, and the welcome screen or main menu should appear.

If the welcome screen or main menu of the console still does not pop up, please check the connection of the cables and the settings of the terminal simulation program.



- **Utilities for network debugging**

The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follows:


Please select utility:
PING Ping host(IP)
Trace Trace routing path
ShowIF Display interface settings
ShowRT Display routing table
ShowARP Display ARP table
Tcpdump sniff on interface
UpTime Display system up time
Status Check service status
Safe Set device into 'safe mode'
NTP Synchronize clock with NTP server
DMESG Print the kernel ring buffer
Main Main menu
< OK >
<Cancel>

- Ping host (IP): By sending ICMP echo request to a specified host and waiting for the response to test the network status.
- Trace routing path: Trace and inquire the routing path to a specific target.
- Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and Netmask.
- Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
- Display ARP table: The internal ARP table of the system is displayed.
- Sniff on interface: This is used to confirm if data packets are passing through the interface.
- Display system up time: The system life time (time for system being turned on) is displayed.
- Check service status: Check and display the status of the system.
- Set device into “safe mode”: This is used if the administrator is unable to use Web Management Interface via browser when the system fails inexplicitly. The administrator can choose this utility and set it into safe mode, which enables him to manage this device with browser again.
- Synchronize clock with NTP server: Immediately synchronizes the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, we must reset the internal clock through the NTP.
- Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their boot-up messages instead of copying the messages by hand.
- Main menu: Go back to the main menu.

- **Change admin password**

Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, we do not need to enter administrator's password to enter the console management interface.

The username and password is needed instead when connecting the system by SSH.

The username is "admin" and the default password is also "admin", which is the same as for the web management interface. Password can also be changed here. If administrators forget their password and are unable to log in to the management interface from the web or the remote end of the SSH, they can still use the null modem to connect to the console management interface and set the administrator's password again.

Caution:

Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the RAYTALK RA-696 Admin username and password after your first login to the system.

- **Reload factory default**

Choosing this option will reset the system configuration to factory defaults.

- **Restart the RAYTALK RA-696**

Choosing this option will restart the RAYTALK RA-696.

11 System Status and Reports

11.1 Viewing the Status

This section includes **System**, **Interface**, **Routing Table**, **Current Users**, **Session List, User Logs, Logs, DHCP Lease** and **Report & Notification** to provide system status information and online user status.

11.1.1 System Status

To view System Status, go to: ***Status >> System***.

This section provides an overview of the system for the administrator.

System Setting Overview		
Up Time		2:18
Firmware Version		2.00.00
Build		1.18-1.5489.2.90
System Name		Wireless Hot Spot Access Point
Portal URL		http://www.google.com
SYSLOG server 1		N/A:N/A
SYSLOG server 2		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
SNMP		Disabled
User Logs	**Retained Days**	3 days
	Receiver's E-mail Address(es)	receiver@gmail.com
		N/A
		N/A
		N/A
		N/A
System Time	**NTP Server**	tock.usno.navy.mil
	Time	2012/06/22 13:01:43 +0800
User Session Control	**Idle Time Out**	10Min(s)
	Multiple Login	Disabled
DNS	**Preferred DNS Server**	N/A
	Alternate DNS Server	N/A

The description of the above-mentioned table is as follows:

Item		***Description***
Up Time		The total time system has operated
Firmware Version		The present firmware version of the RAYTALK RA-696
Build		The present build number of the firmware
System Name		The system name. The default is Wireless Hotspot Access Point
Portal URL		The page users are directed to after initial login success
SYSLOG server- System Log		The IP address and port number of the external SYSLOG Server. **N/A** means that it is not configured
SYSLOG server- On-demand Users Log		The IP address and port number of the external SYSLOG Server. **N/A** means that it is not configured
Proxy Server		Shows status of built-in Proxy Server
Warning of Internet Disconnection		Shows whether the status for the connection at WAN is normal or abnormal (**Internet Connection Detection**) and all online users are allowed/disallowed to log in the network
SNMP		Shows status of option to enable or disabled system info retrieval via SNMP protocol
User Log		The maximum number of days for the system to retain the users' information
SNMP		The email address to which the user log information will be sent
System Time	**NTP Server**	The network time server that the system is set to align
	Time	The system time is shown as the local time
User Session Control	**Idle Time Out**	The minutes allowed for the users to be inactive before their account expires automatically
	Multiple Login	Enabled/disabled stands for the current setting to allow/disallow multiple login from the same local account
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server
	Alternate DNS Server	IP address of the alternate DNS Server

11.1.2 Interface Status

To view Interface Status, go to: *Status>> Interface.*

This section provides an overview of the interface for the administrator including WAN, Zone-Private and Zone-Public.

The description of the table is as follows:

Item		***Description***
WAN	**Mode**	Shows WAN interface settings: Static, Dynamic, PPPoE or PPTP
	MAC Address	The MAC address of the WAN port
	IP Address	The IP address of the WAN port
	Subnet Mask	The Subnet Mask of the WAN port
	IPv6 Address	The IPv6 address of WAN port if applicable
	IPv6 Prefix	The IPv6 prefix if applicable
Zone - General	**Mode**	The operation mode of the zone
	MAC Address	The MAC address of the zone
	IP Address	The IP address of the zone
	Subnet Mask	The Subnet Mask of the zone
	IPv6 Address	The IPv6 address of the zone if applicable
Zone - DHCP	**Status**	Enable/disable stands for the status of the DHCP server in this zone
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured
	Start IP Address	The start IP address of the DHCP IP range
	End IP address	The end IP address of the DHCP IP range
	Lease Time	Minutes of lease time of the IP address
Zone - VAP	**BSSID**	The BSSID of this zone
	ESSID	The ESSID of this zone
	Security Type	The current security type of this zone
	Associated Clients	The number of associated clients in this zone

11.1.3 Routing Table

To view System Status, go to: ***Status >> Routing Table***.

All the **Policy** Routing rules and **Global Policy** Routing rules for both IPv4 and IPv6 will be listed here.

It will also show the **System** Routing rules specified by each interface. The following depicts an image for the IPv4 Routing Table.

Policy 1			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Policy 2			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Policy 3			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Policy 4			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Policy 5			
Destination	**Subnet Mask**	**Gateway**	**Interface**

Interface			
Destination	**Subnet Mask**	**Gateway**	**Interface**
192.168.1.0	255.255.255.0	0.0.0.0	Private
192.168.11.0	255.255.255.0	0.0.0.0	Public
169.254.0.0	255.255.0.0	0.0.0.0	Private
10.29.0.0	255.255.0.0	0.0.0.0	WAN

System			
Destination	**Subnet Mask**	**Gateway**	**Interface**
0.0.0.0	0.0.0.0	10.29.0.1	WAN

- **Policy 1~5:** Shows the information of the individual Policy from 1 to 5.
- **Global Policy:** Shows the information on the Global Policy.
- **System:** Shows the information on the system administration.

> **Destination:** The Destination IP address.

> **Subnet Mask:** The Subnet Mask of the IP address range.

> **Gateway**: The Gateway IP address of the interface.

> **Interface:** Including **WAN**, **Private** and **Public**.

11.1.4 Current Users

To view Current Users, go to: ***Status >> Current Users***.

On this page, each online user's information including **Username**, **IP Address**, **MAC Address, IPv6 Address**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out, Service Zone/VLAN, Group/Policy, Authentication Method/Authentication Database**, **Online/Idle** and **Kick Out** will be shown.

Administrators can force out a specific online user by clicking the hyperlink of **Kick Out**.

Click **Refresh** to update the current users list.

Non-Login Devices shows users that have acquired an IP address from the system's DHCP server but have not yet been authenticated, either under the LAN or remotely tunneled site. This feature is designed for administrators to keep track of systems' resources from being exhausted.

The list shows the client's **MAC Address, IP Address** and associated **VLAN ID,** as well as the **Service Zone**.

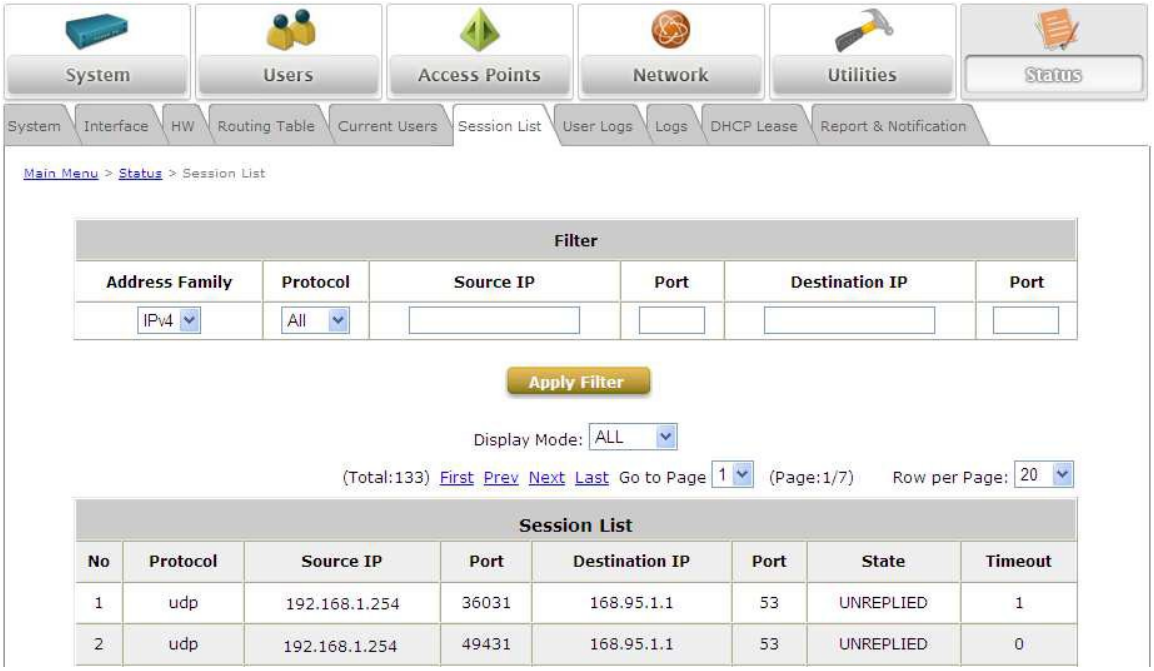
The **On-demand Roaming Out User List** shows the users that are authenticated by other gateways using this RayTalk RA-696's On-demand database as RADIUS database.

11.1.5 Session List

This page allows the administrator to inspect sessions currently established between a client and the system.

Each result displays the IP and Port values of the Source and Destination.

You may define the filter conditions and display only the results you desire.



11.1.6 User Log

To view User Log, go to: ***Status >> User Log***.

This page is used to check the traffic history of the RayTalk RA-696.

The history of each day will be saved separately in the RAM memory for at least 3 days (72 full hours).

The system also keeps a cumulated record of the traffic data generated by each user in the last 2 calendar months.

Users Log	
Date	**Size (Byte)**
2012-07-10	131
2012-07-09	131
2012-07-08	131

On-demand Users Log	
Date	**Size (Byte)**
2012-07-10	186
2012-07-09	186
2012-07-08	186

Roaming Out User Log	
Date	**Size (Byte)**
2012-07-10	106
2012-07-09	106
2012-07-08	106

Roaming In User Log	
Date	**Size (Byte)**
2012-07-10	173
2012-07-09	173
2012-07-08	173

Monthly Network Usage of Local User		
Month	**No. of Entries**	**Usage Data**
2012-07	0	Download
2012-06	0	Download

Caution:

Since the history is saved in the RAM memory, if you need to restart the system at the same time, please keep the history, manually by copying and saving the traffic history information before restarting.

If the **Receiver E-mail Address(es)** has been entered under the **Notification Settings** page, the system will automatically send out these history information to that specified email address.

- **Users Log**

All user activities on the system within 72 hours excluding other user logs such as On-demand user log are recorded; in date and time order. Each line is a traffic history record consisting of 17 fields, including **Date**, **Type, Name**, **IP**, **IPv6, MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out**, and other information of the user activities.

- **On-demand User Log**

Each line is a on-demand user log record consisting of 25 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, Activation Time, 1st Login Expiration Time**, **Remark,** and other information, of On-demand user activities are included.

- **Roaming Out User Log**

Each line is a roaming out traffic history record consisting of 14 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

- **Roaming In User Log**

Each line is a roaming in traffic history record consisting of 22 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out**, **Message**, and other information of user activities are included.

11.1.7 Local User Monthly Network Usage Report

To view Local User Monthly Network Usage, go to: ***Status >> User Log***.

- **Monthly Network Usage of Local User**

The system keeps a cumulated record of the traffic data generated by each Local user in the last 2 calendar months.

Each line in the 'Monthly Network Usage of Local User' record (hyperlinked) consists of 6 fields, **Username**, **Connection Time Usage**, **Packets In**, **Bytes In**, **Packets Out** and **Bytes Out** of user activities.

o **Username:** Username of the local user account.

o **Connection Time Usage:** The total time used by the user.

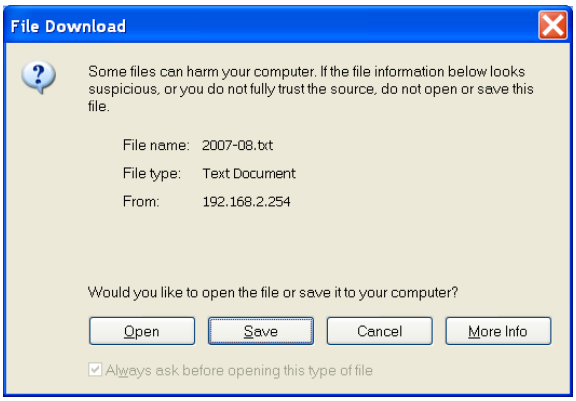
o **Pkts In/ Pkts Out:** The total number of packets received and sent by the user.

o **Bytes In/ Bytes Out:** The total number of bytes received and sent by the user.

> **Download Monthly Network Usage of Local User:** Click the ***Download*** button for outputting the report manually to a local database.

Monthly Network Usage of Local User		
Month	**No. of Entries**	**Usage Data**
2009-04	1	Download

A warning message will then appear. Click ***Save*** to download the record into .txt format.


File Download
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.
File name: 2007-08.txt
File type: Text Document
From: 192.168.2.254
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

11.1.8 System Related Logs

To configure System related logs, go to: ***Status >> Logs***.

This page displays the system's local log information since system boot up.

Administrators can examine the log entries of various events.

However, since all these information are stored on volatile memory, they will be lost during a restart/reboot operation.

Therefore if the log information needs to be documented, the administrator will need to make back up manually.

Logs	
System Log	Show
Web Log	Show
UAMD Log	Show
RADIUS Server Log	Show
On-demand User Billing Report Log	Show
Configuration Change Log	Show

- **System Log**

This page displays system related logs for event tracing.

- **Web Log**

This page shows which of the web pages have been accessed on the RayTalk RA-696's built-in web server.

- **UAMD Log**

This page displays the UAM related information output from the UAM daemon.

- **RADIUS Server Log**

This page displays the RADIUS messages that pass through the MiMo Hot Spot Access Point Wi-Fi RayTalk RA-696.

- **On-demand Billing Report Log**

This page displays a summary of On-demand account transactions.

- **Configuration Change Log**

This page shows the account and IP of the user that has made configuration changes to the RayTalk RA-696.

11.1.9 DHCP Lease

To configure DHCP Lease related logs, go to: ***Status >> DHCP Lease***.

The DHCP IP lease statistics can be viewed after clicking on ***Show*** Statistics List in this page.

- **Statistics of offered list**

Valid lease counts of the **Last 10 Minutes, Hours** and **Days** are shown here. The header 1 ~ 10 are the unit multipliers.

For instance the number under column 2 indicates the lease count in the last 20 minutes/hours/days, the number under column 3 indicated the lease count in the last 30 minutes/hours/days and so on.

- **Statistics of expired list**

IP leased to clients that have expired in the **Last 10 Minutes, Hours** and **Days** are shown here. The header 1 ~ 10 are the unit multipliers. For instance the number under column 2 indicates the expired count in the last 20 minutes/hours/days, the number under column 3 indicates the expired count in the last 30 minutes/hours/days and so on.

Statistics of offered list

	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	1	0	0	0	0	0	0	0	0	0
Last 10 Hours	0	2	22	3	1	0	0	1	2	2
Last 10 Days	51	0	0	0	0	0	0	0	0	0

Statistics of expired list

	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	0	0	0	0	0	0	0	0	0	0
Last 10 Hours	0	0	1	0	0	0	0	0	2	1
Last 10 Days	10	0	0	0	0	0	0	0	0	0

Refresh Refresh Disable

- **DHCP Lease List**

Valid IP addresses issued from the DHCP Server and related information of the client using this IP address is displayed here.

11.2 Notification

To configure Notification, go to: ***Status >> Report & Notification***.

The RAYTALK RA-696 can automatically send the notifications of **Monitor IP Report**, **Users Log**, **On-demand User Log**, **Roaming Out Users Log**, **Roaming In Users Log**, **Firewall Log**, **Session Log** and **On-demand User Billing Report** to up to 5 particular e-mail addresses.

A trial email is provided by the system for validation.

Secondly, the system supports recording of **Users Log**, **On-demand Users Log**, **Roaming Out Users Log**, **Roaming In Users Log**, **Session Log**, **Firewall Log**, and **Local HTTP Web Log, HTTP Web Log** and **DHCP Server Log** via external SYSLOG servers.

Thirdly, **Users Log**, **On-demand Users Log**, **Roaming Out Users Log**, **Roaming In Users Log**, **Session Log**, **On-demand User Billing Report**, **Local HTTP Web Log**, **HTTP Web Log**, **WMI Configuration Log**, **DHCP Lease Log** and **Traffic Report** can also be configured to be sent to an external FTP server.

In addition, the **Event Log** section on WMI displays clients associate and disassociate messages.

11.2.1 E-Mail

SMTP Settings	
Receiver E-mail Address 1	
Receiver E-mail Address 2	
Receiver E-mail Address 3	
Receiver E-mail Address 4	
Receiver E-mail Address 5	
Sender E-mail Address	*
SMTP Server	*
SMTP Port	25 *
SMTP over SSL	Enable Disable
SMTP Authentication	None

- **SMTP Settings:**

> **Receiver Email Address (es):** Up to 5 e-mail addresses can be set up to receive the notification.

There are eight kinds of notification for selection -- Monitor IP Report, Users Log, On-demand Users Log, Roaming Out Users Log, Roaming In Users Log, Session Log, Firewall Log, and On-demand Billing Report, check the selection box to choose the type of notification to be sent.

> **Sender Email Address:** The e-mail address of the administrator in charge of monitoring. This will show up as the sender's e-mail.

> **SMTP Server:** The IP address of the sender's SMTP server.

> **SMTP over SSL:** Enable or Disable SMTP over SSL for additional security

> **SMTP Authentication:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method is selected, enter the **Account Name**, **Password** and **Domain**.

  - **NTLMv1** is not currently available for general use.
  - **Plain** and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**. Outlook and Outlook express use **Login** as default, although they can be set to use **NTLMv1**.
  - Pegasus uses **CRAM-MD5** or **Login** however the method to be used cannot be configured.

- **Notification E-mail Settings:**

> **Receiver Email Address (es):** Up to 5 e-mail addresses can be set up to receive the notification. There are eight kinds of notification for selection -- Monitor IP Report, Users Log, On-demand Users Log and Session Log, check the selection box to choose the type of notification to be sent.

> **Interval:** The time interval to send the e-mail report.

11.2.2 SYSLOG

- **SYSLOG Server Settings:** There are 9 types of SYSLOG supported: **Users Log**, **On-demand Users Log**, **Roaming Out Users Log**, **Roaming In Users Log**, **Session Log**, **Firewall Log**, **Local HTTP Web Log**, **HTTP Web Log** and **DHCP Server Log**. Enter the IP address and Port number to specify the SYSLOG server where the report should be sent to.

Except for System Log, each supported log may be assigned *Tag* information as well as SYSLOG standard attributes *Severity* to meet the filtering requirements on the SYSLOG Server. HTTP Web Log can further select which Service Zone Web interface information to log. For each type of log information, whenever an incident occurs and data is updated, the updated log will be immediately sent to the configured SYSLOG server.

Note:

When the number of a user's session (TCP and UDP) reaches the session limit specified in the policy, a record will be logged to this SYSLOG server.

11.2.3 FTP

This configuration page allows the setting of FTP Server to send, including the types of Roaming Out Users Log, Roaming In Users Log, On-demand User Billing Report, Session Log, Local HTTP Web Log, HTTP Web Log, WMI Configuration Log, DHCP Lease Log, Traffic Report, User Log or On-demand User Log based on Server Folder and Interval.

- **FTP Server Settings**

FTP Destination: Configures the common settings of the FTP server that the logs will be sent to. Further settings can be configured under **Notification Settings**, which includes the following:

> **IP Address/Port:** IP address and port number of FTP server.

> **Anonymous:** Check option "Yes" if the FTP server does not need ID credentials, otherwise check option "No" and fill in the necessary *Username* and *Password*.

> **FTP Setting Test:** To test if the FTP settings are correct or not.

> **User Log:** Records the User Log of the system to a specific FTP server.

> **On-demand User Log:** Records the On-demand User Log of the system to a specific FTP server.

> **Roaming Out / In Users Log:** Records the Roaming Out / In Users Log to a specific FTP server.

> **Session Log:** Log each connection created by users and track the source IP/Port and destination IP/Port. Session Log will be sent to the FTP server automatically in every defined interval in Session Log email notification. Session Log allows uploading the log file to a FTP server periodically. The maximum log file size is 256K. The log file will also be sent to the FTP server once the file size reaches its maximum size.

> **On-demand User Billing Report:** Records the On-demand User Billing Report to a specific FTP server.

> **Local HTTP Web Log / HTTP Web Log:** Records the URL of websites visited by users accessing the internet via the RAYTALK RA-696 to a specific FTP server.

> **WMI Configuration Log:** Records the WMI Configuration Log of the system to a specific FTP server.

> **DHCP Lease Log:** Records the DHCP Lease Log of the system to a specific FTP server.

> **Traffic Report:** Records the Traffic Report of the system to a specific FTP server.

Notification Settings

	Receiver E-mail Address(es)						SYSLOG	FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	☐	☐	☐	☐	☐	Detail / Send	N/A	N/A	1 Hour
Users Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour
On-demand Users Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour
Roaming Out Users Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour
Roaming In Users Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour
Session Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	☐ Detail	1 Hour
Firewall Log	☐	☐	☐	☐	☐	Detail / Send	☐ Detail	N/A	1 Hour
On-demand User Billing Report	☐	☐	☐	☐	☐	Detail / Send	N/A	☐ Detail	☐ Daily Settle Time 0 ☐ Weekly Settle Time Sun ☐ Monthly Settle Time 1
Local HTTP Web Log	N/A						☐ Detail	☐ Detail	1 Hour
HTTP Web Log	N/A						☐ Detail	☐ Detail	1 Hour
WMI Configuration Log	N/A						N/A	☐ Detail	1 Hour
DHCP Server Log	N/A						☐ Detail	N/A	N/A
DHCP Lease Log	N/A						N/A	☐ Detail	1 Hour
Traffic Report (Text) ☐ Service Zone	N/A						N/A	☐ Detail	1 Hour

> **Server Folder:** The folder in the configured FTP Server in which the sent Log will be placed.

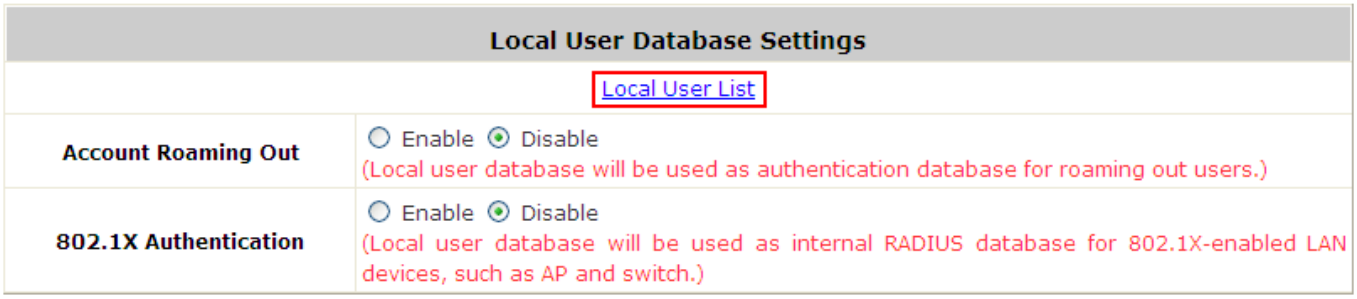
> **Interval:** The time interval at which the Log will be sent.

> **Logged Interface:** The check box of Public or Private shall be checked to enable logging the HTTP Web Log of this interface.

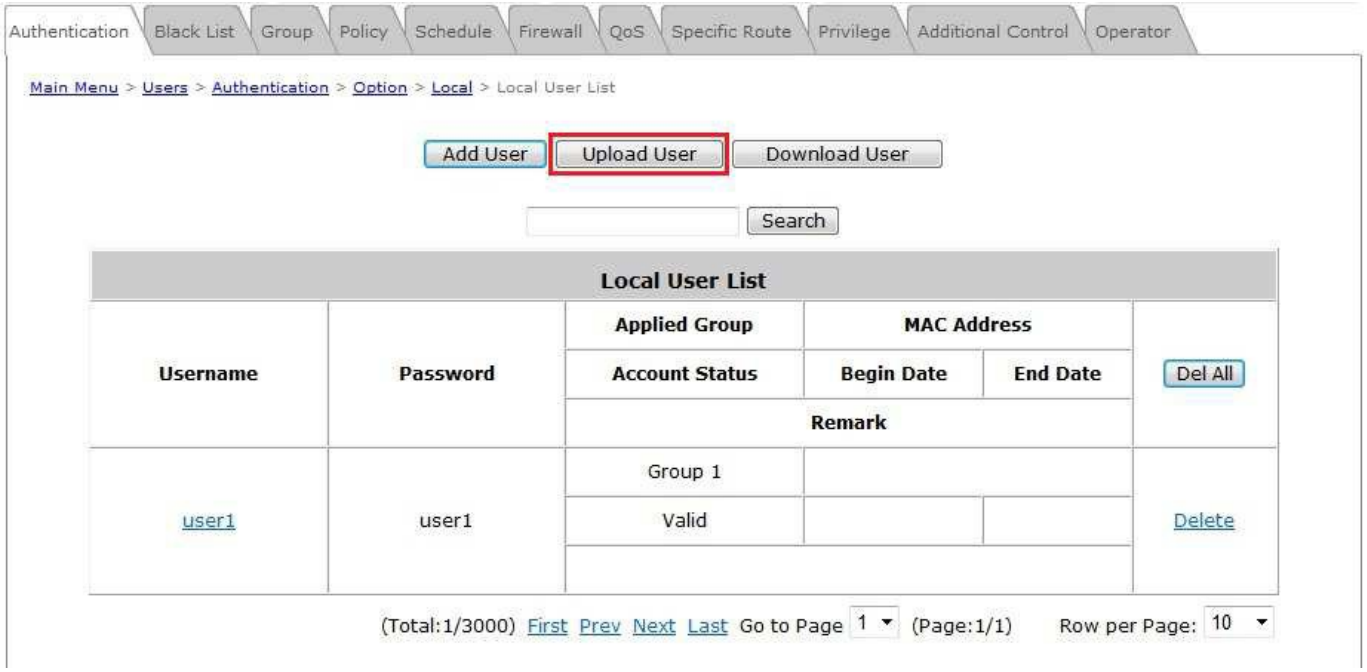
12 Advanced Applications

12.1 Upload/Download Local User Accounts

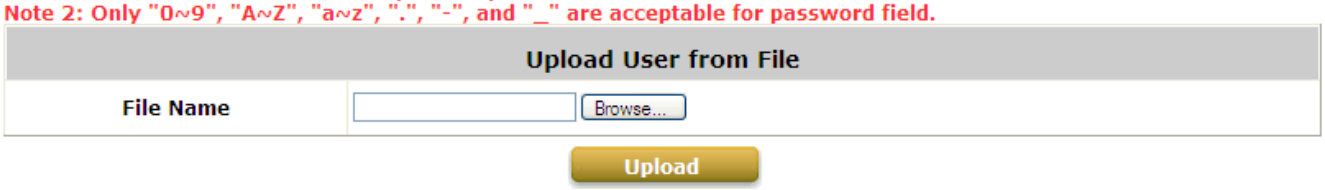
To Upload / Download Local Users Accounts, go to: ***Users >> Authentication,*** click ***Configure*** for the ***Local*** Authentication Database. Or click ***Quick Links >> Local User Management*** from system Home page.


Local User Database Settings
Local User List
Account Roaming Out
Enable Disable
(Local user database will be used as authentication database for roaming out users.)
802.1X Authentication
Enable Disable
(Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)

- **Upload User:** Click **Upload User** to enter the **Upload User from File** interface. Click the ***Browse*** button to select the text file for uploading user accounts, then click **Upload** to complete the upload process.

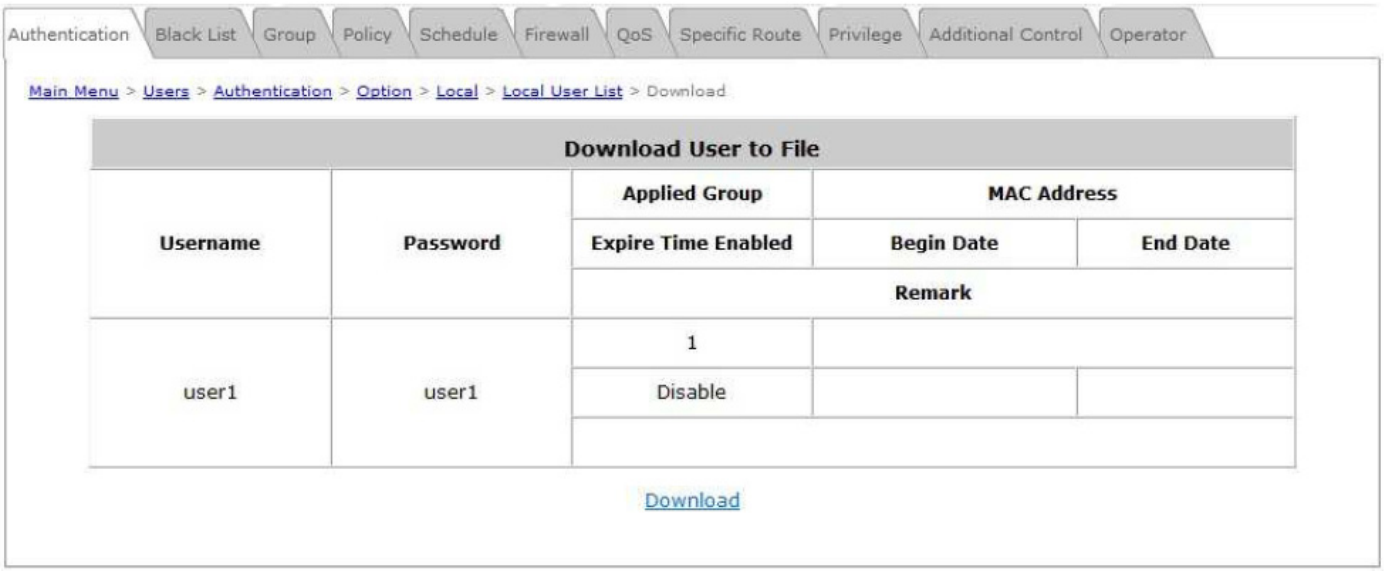


Note 1: The format of each line is "Username, Password, MAC Address, Applied Policy, Remark" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.
Note 2: Only "0~9", "A~Z", "a~z", ".", "-", and "_" are acceptable for password field.



When the system uploads a file, any format error or duplicated username will terminate the uploading process and no account will be uploaded. Please correct the format in the uploading file or delete the duplicated user accounts in the database then try again.

- Download User: Use this function to create a .txt file with all *Local* user account information and save it on a disk.



12.2 RADIUS Advanced Settings

To configure RADIUS Advanced Settings, go to: ***Users >> Authentication***. Click ***Configure*** for the ***RADIUS*** Authentication Database.

> **Complete vs. Only ID vs. Leave Unmodified**

For RADIUS authentication, there is an option to send the complete username with postfix or username only.

Username Format: When the **Complete** option is checked, both the username and postfix will be transferred to the RADIUS server for authentication.

On the other hand, when the **Only ID** option is checked, only the username will be transferred to the external RADIUS server for authentication.

If the **Leave Unmodified** option is selected, the system will send the username to **Default Auth Server** set in **802.1X** configuration page for authentication.

> **NAS Identifier**

System will send this value to the external RADIUS server, if needed by the external RADIUS server.

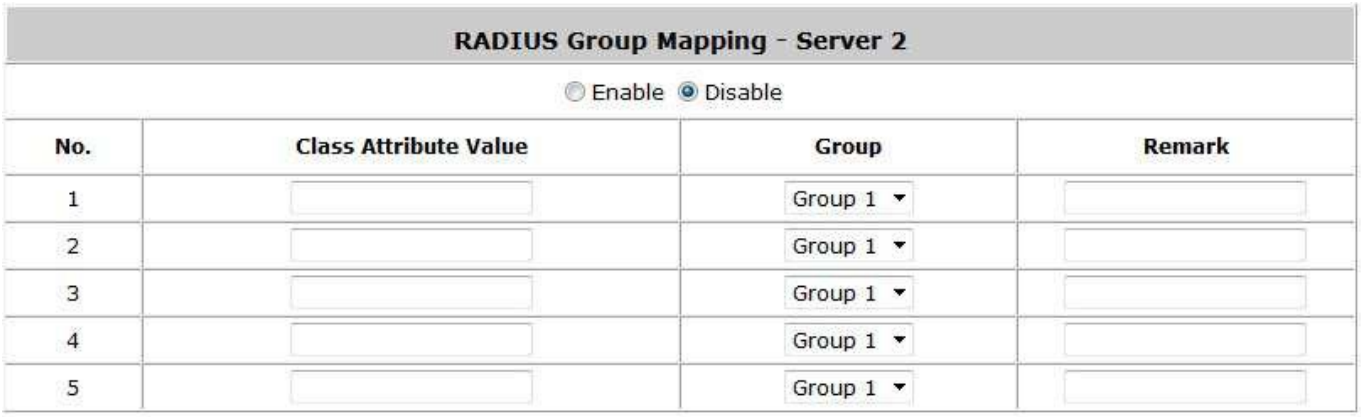
> **NAS Port Type**

System will send this value to the external RADIUS server, if needed by the external RADIUS server.

> **Class-Group Mapping**

This function is to assign a *Policy* to a RADIUS class attribute sent from the RADIUS server.

When the clients classified by RADIUS class attributes log into the system via the RADIUS server, each client will be mapped to its assigned Group and Policy.



12.3 Roaming Out

To configure local user Roaming Out, go to: ***Users >> Authentication,*** *click* ***configure*** *for* ***Local***.

Under certain configurations, the RAYTALK RA-696 can act as a RADIUS server for Roaming Out local users logged from another system.

The Local User database will act as the RADIUS user database.

- **Account Roaming Out & 802.1X Authentication:** When Account Roaming Out is enabled; the link of *Roaming Out & 802.1X Client Device Settings* will be available to define the client device authorized to roam by entering the IP address, Subnet Mask, and Secret Key.

Local User Database Settings	
Local User List	
Account Roaming Out	(•) Enable ( ) Disable (Local user database will be used as authentication database for roaming out users.)
802.1X Authentication	( ) Enable (•) Disable (Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
RADIUS Client Device Settings	

802.1X Auth Setting	
Default Auth Server	Server 1 (Postfix: local) (The Auth server is for username only with ID, e.g. user1.)

RADIUS Client Device Settings					
No.	**Type**	**IP Address**	**Subnet Mask**	**Secret Key**	**SNMP Community**
1	Roaming Out	127.0.0.0	255.0.0.0 (/8)	••••••••	
2	Disable		255.255.255.255 (/32)		
3	Disable		255.255.255.255 (/32)		
4	Disable		255.255.255.255 (/32)		
5	Disable		255.255.255.255 (/32)		

Click the hyperlink ***Roaming Out & 802.1x Client Device Settings*** to enter the ***Roaming Out & 802.1X Client Device Settings*** interface.

Choose **Roaming Out** and enter the Roaming Out client's IP address and network mask and then click ***Apply*** to complete the settings.

12.4 Customizable Pages

To configure Custom Pages, go to: ***System >> Service Zones,*** *click* ***Configure*** *in* ***Public*** *zone*.

There are several user login and logout pages that can be customized by the administrator.

You can select **Default Page, Template Page, Uploaded** or **External Page**.

Custom Pages	Disclaimer Page	Configure
	Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Failed Page	Configure
	Login Success Page for On-demand User	Configure
	Logout Success Page	Configure
	Logout Failed Page	Configure

- **Disclaimer Page**:

The **Disclaimer Page** is for the hotspot owner or MIS staff who wants to display 'terms of use" or announcement information before the user login page.

Click ***Configure***, the setup page will appear. An unauthorized client will receive a disclaimer page once opening the web browser. If a client selects "I agree" and clicks **Next**, then he or she will proceed to the User Login Page for client to login with username and password. The Disclaimer Page can be Enabled at: **System >> General**

- **Template Page:**

To utilize the template user pages stored locally in the system, choose ***Template Page*** and configure the necessary settings as follows.

Click ***Select*** (hyperlinked) to pick up a color for each item and fill in your copyright message. You can also upload a Logo image file for your template with the ***Preview and Edit the Image File*** button.

Click ***Configure***, the setup page will appear for the corresponding page where you can change the text displayed as you wish. After setting is finished, click ***Preview*** to see the result. If you are happy with the customized pages, click ***Apply*** to activate the changes made.

- **Uploaded Page:**

Choose the ***Uploaded Page*** option if you wish to upload your own html coded page.

Click ***Configure*** for each custom page and upload the HTML file and corresponding image files and click ***Apply***.

After applying the setting, the new login page can be previewed by clicking ***Preview*** button.

- **External Page:**

Choose the ***External Page*** option if you wish to use user pages located on a designated website.

Click ***Configure*** for each custom page and enter the URL of its corresponding external login page and click ***Apply***.

After applying the setting, the new login page can be previewed by clicking ***Preview*** button.

Appendix A. Policy Priority

Global Policy, Authentication Policy and User Policy

The RAYTALK RA-696 supports multiple Policies, including one **Global Policy** and 5 individual **Policies** can be assigned to different **Authentication Server**. **Global Policy** is the system's universal policy and is applied to all clients, while other individual Policies can be selected and defined to be applied to any Authentication Server.

For some authentication, such as Local and RADIUS, users can be assigned to different Policies individually.

One user may be applied to a different policy at the same time.

Which policy is actually applied to this user?

The Policy Priority is enforced as follows:

User Policy >> Authentication Policy >> Global Policy

Now, let us discuss the different user policy types:

> For Local and RADIUS, users can be assigned to different policies individually.

For example, a Local user, user01, is assigned to Policy1 and the Local Authentication Policy2.

When user01 logs in to Public Zone, user01 will be governed under Policy1.

This is a common case for users that can be assigned a Policy individually.

> For Local and RADIUS, if these users are not assigned under any User Policy individually, they will be governed under the same policy as others within the same authentication server.

For example, if the Local Authentication is assigned to Policy3, a Local user01 when logged in to Public Zone will get Policy3.

This is another common case for users that are assigned Policy by the authentication server.

> If a User is not assigned a Policy individually and the authentication server is also not assigned a Policy, then the Global Policy will be applied to all users.

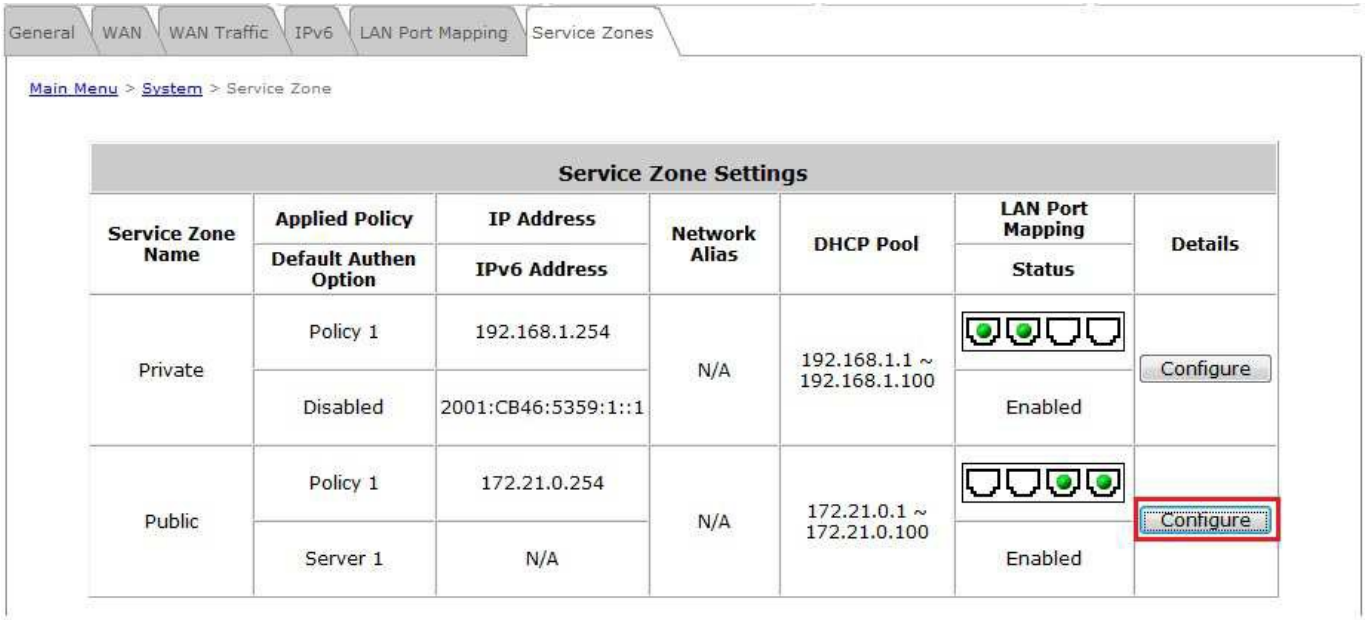
For example, a Local user, user01, is assigned to *None* Policy and the Local Authentication is also assigned to *None Policy* on User list. Then user01 logged in to Public Zone will be applied with the Global Policy.

In conclusion, the Global Policy has the lowest policy priority; the User Policy has the highest priority.

Appendix B. WDS Management

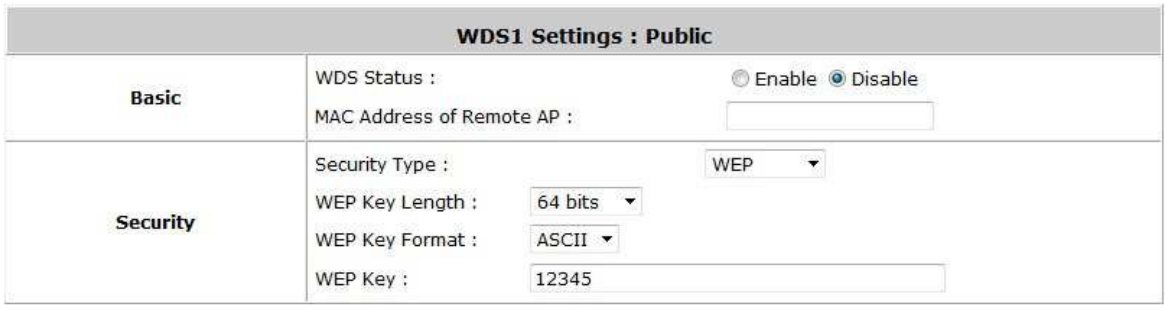
The Public Zone of the RAYTALK RA-696 supports up to 2 WDS links. WDS (Wireless Distribution System) is a function used to connect APs (Access Points) wirelessly to extend wireless coverage.

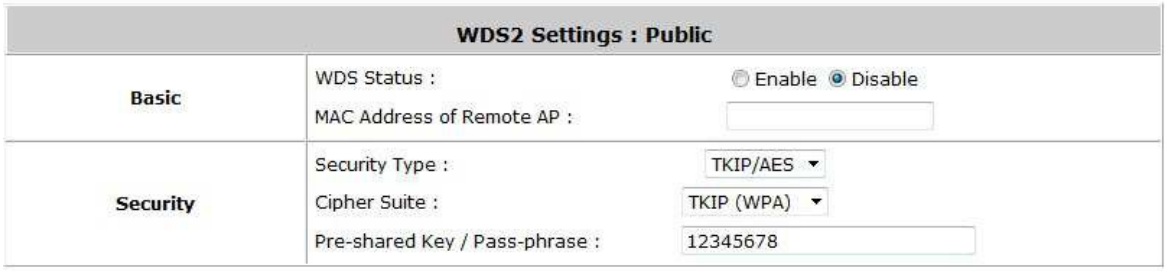
The WDS management function of the system can help administrators to setup two WDS links. To configure WDS, go to: ***System >> Service Zones,*** *click* ***Configure*** *in* ***Public*** *zone*.



WDS (Wireless Distribution System) is a function used to connect **AP**s (Access Points) wirelessly.

The WDS management function of the system can help administrators to setup two WDS links.


WDS1 Settings : Public
Basic
WDS Status : Enable Disable
MAC Address of Remote AP :
Security
Security Type : WEP
WEP Key Length : 64 bits
WEP Key Format : ASCII
WEP Key : 12345


WDS2 Settings : Public
Basic
WDS Status : Enable Disable
MAC Address of Remote AP :
Security
Security Type : TKIP/AES
Cipher Suite : TKIP (WPA)
Pre-shared Key / Pass-phrase : 12345678

- **WDS Status:** Select ***Enable*** to activate this WDS link.
- **MAC Address of Remote AP:** Enter the MAC of the remote AP that generates a WDS link with the RayTalk RA-696.
- **Security Type:**
    - **WEP: WEP Key Length** may be *64 bits*, *128 bits* or *152 bits*; and **WEP Key Format** can be *ASCII* or *HEX*. Enter the applicable **WEP Key**.
    - **WPA-PSK:** Select the preferred ciphering method, *TKIP* or *AES* and enter the **PSK / Pass-phrase**.

Appendix C. RADIUS Accounting

This section will briefly introduce the basic configuration of RADIUS server to work with VSA for controlling the maximum client volume usage (upload; download or upload + download traffic).

This **VSA** will be sent from the RADIUS server to the gateway along with an **Access-Accept** packet.

In other words, when the external RADIUS server accepts the request, it will reply not only an **Access-Accept** but also a maximum value in bytes each user is allowed to transfer.

This value can be the maximum upload traffic, the maximum download traffic, or the sum of the download and upload traffics in bytes per user.

The gateway will check this value every minute; if the user traffic reaches this value, the gateway will stop the session of this user and send a "Stop" to RADIUS server.

1. Description

VSA is designed to allow vendors to support their own extended Attributes which are not covered in common attributes.

It MUST not affect the operation of the RADIUS protocol.

"**Attribute Number**" and "**Attribute Value**" can then be designed to provide additional control over RADIUS.

If the amount of traffic is larger than 4 GB, the attributes of "XXXX-4GB" will be used.

On the other hand, when the administrator fills in all attributes, the user will be kicked out from the system if any condition is reached.

2. VSA configuration in RADIUS server (IAS Server)

This section will guide you through a VSA configuration in your external RADIUS server.

Before getting started, please directly or remotely access your external RADIUS server's desktop from other PC.

Step 1

Confirm the following key elements in the RADIUS server: users, groups, and policies.

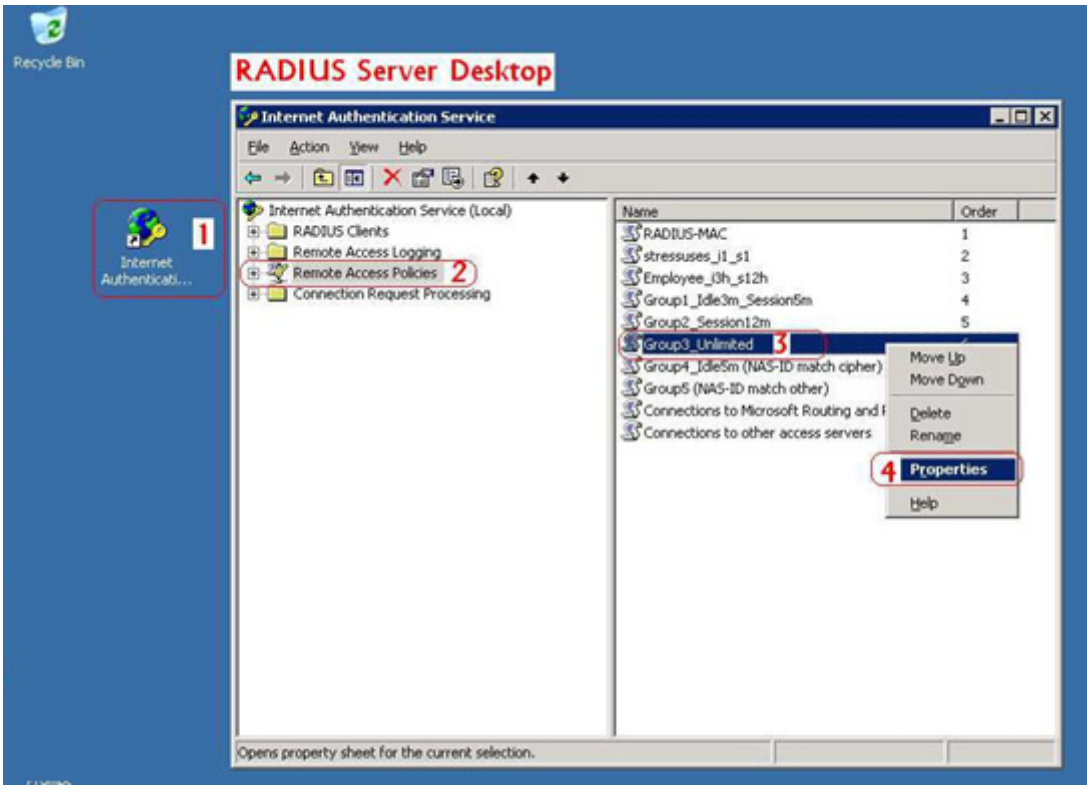
Verify whether there are already **users** in the RADIUS Server.

Verify whether there are already **Groups** and assigned **users** belonging to these **Groups** in the RADIUS Server.

Verify whether there are already **Policies** and assigned **Groups** belonging to these **Policies** in the RADIUS Server.

Step 2

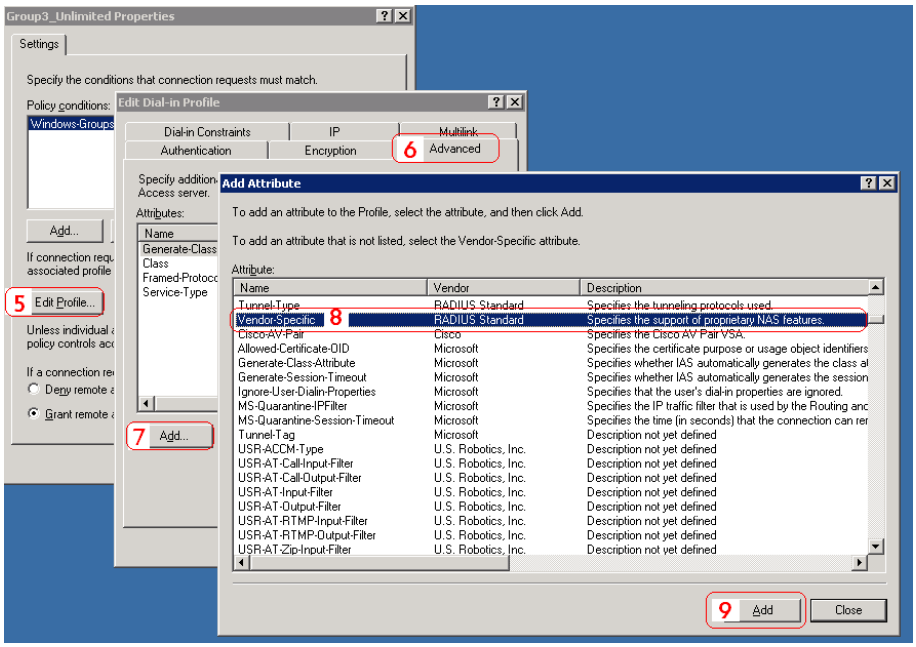
Run “Internet Authentication Server” and open “Remote Access Policies” Right-click



Policy and scroll down to the **Properties** page.

Step 3

Click **Edit Profile and** select the **Advanced** Tag. Click **Add** to add a new **Vendor-specific** attribute.



Step 4

Add a new attribute under **Vendor-specific**

Check **Yes** to conform to the RADIUS RFC. Click **Configure Attribute** to proceed.

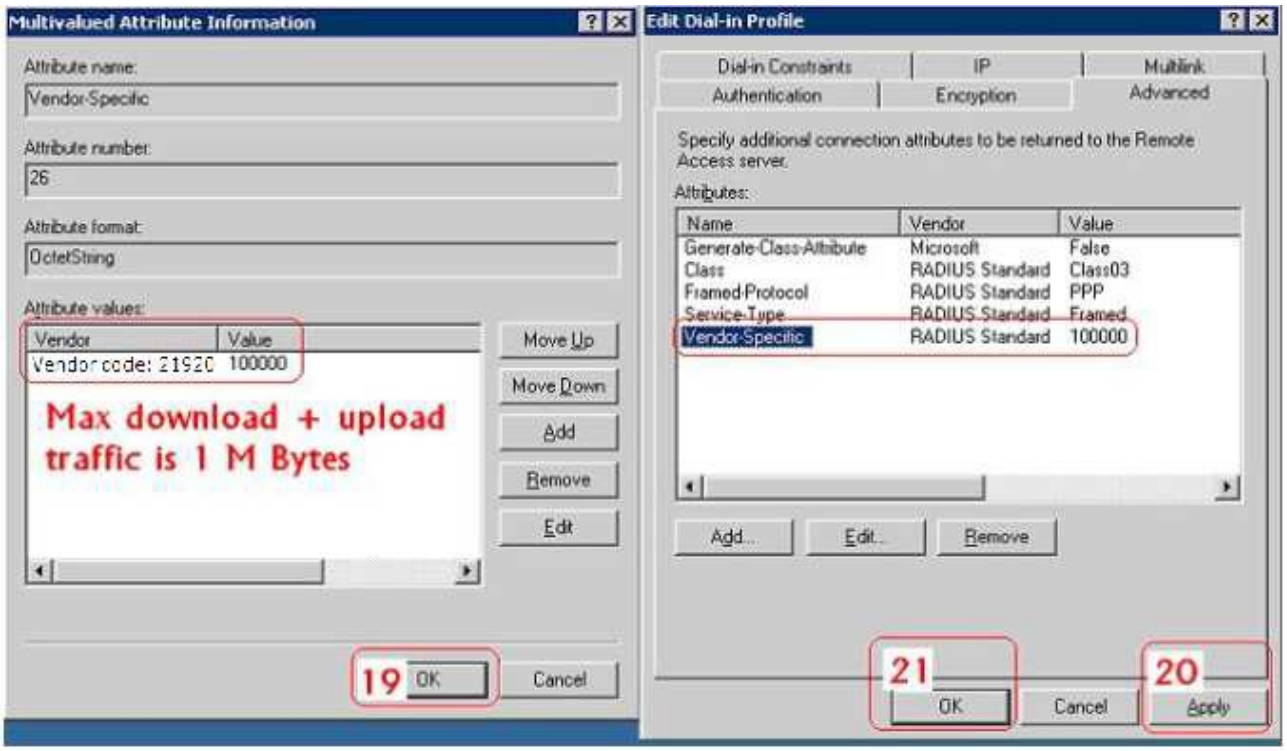
Set **"Vendor-assigned attribute number = 10"**

Select **"Attribute format = Hexadecimal"**

Set **"Attribute Value = 1000000"**

Step 5

Confirm whether the **Vendor-specific Attribute** has been added successfully



Step 6

Follow the same steps to create other **Vendor-specific Attributes** if needed.

3. VSA configuration in RADIUS server (FreeRADIUS)

This section will guide you through **VSA** configuration with FreeRADIUS v1.0.5 running on "Fedora". Before getting started, open the shell of RADIUS server; for example, use *Putty* to access the Linux host:

Step 1

Confirm the following key elements in the RADIUS server: users, groups

Verify whether there are already **users** in the RADIUS Server.
Verify whether there are already **Groups** and assigned **users** belonging to these **Groups** in the RADIUS Server.

Step 2

Log in to the Linux host of the RADIUS server.

Step 3

Create a file under the "freeradius" folder.

Step 4

Edit and save the contents of the file as follows:

```
VENDOR                          21920

#
#       Standard attribute
#
ATTRIBUTE               -Byte-Amount                10      interger
```

Administrator can also add other attributes as the table stated in Section 2 with the same format.

```
VENDOR                          21920

#
#       Standard attribute
#
ATTRIBUTE               -Byte-Amount                10    interger
ATTRIBUTE               -MaxByteIn                  11    interger
ATTRIBUTE               -MaxByteIn                  12    interger
ATTRIBUTE               -Byte-Amount-4GB            20    interger
ATTRIBUTE               -MaxByteIn-4GB              21    interger
ATTRIBUTE               -MaxByteIn-4GB              22    interger
```

Step 5

Edit the file under the folder "freeradius".

Step 6

To include "the file in the dictionary of RADIUS server, insert it in an incremental position as follows.

```
$INCLUDE dictionary.ascend
$INCLUDE dictionary.bay
$INCLUDE dictionary.bintec
$INCLUDE dictionary.cabletron
$INCLUDE dictionary.
$INCLUDE dictionary.cisco
#
#  This is the same as the altiga dictionary.
#
#$INCLUDE dictionary.cisco.vpn3000
$INCLUDE dictionary.cisco.vpn5000
$INCLUDE dictionary.cisco.bbsm
$INCLUDE dictionary.colubris
$INCLUDE dictionary.erx
```

Step 7

Open the “radius” database.

```
[vivian@linux ~]$ mysql -u root -p radius
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 98 to server version: 5.0.27

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Step 8

Insert **VSA** into RADIUS response. In this example, the maximum download and upload traffics in bytes for **group03 users** is 1MBytes.

```
mysql> INSERT INTO radgroupreply (GroupName,Attribute,op,Value)
VALUES ('group03', cipherium-Byte-Amount',':=','1048576')
Query OK, 1 row affected (0.00 sec);
mysql> exit
Bye
```

Step 9

Restart RADIUS daemon to get your settings activated.

```
[vivian@linux ~] # /etc/init.d/radiusd restart
Stopping RADIUS server:                                    [  OK  ]
Starting RADIUS server: Thu Oct 30 14:26:41 2008 : Info: Starting - reading conf
iguration files ...
                                                           [  OK  ]
```

Appendix D. On-demand Account types & Billing Plan

This section explains the parameters as well as the different account types provided when editing billing plans in On-demand authentication.

Usage-time with Expiration Time: Users can access internet as long as account is valid with remaining quota (usable time). Users need to activate the purchased account within a given time period by logging in. It is Ideal for short-term usage, namely in coffee shops, at airport terminals, etc. This billing type only deducts quota when internet is being used. However, the countdown to Expiration Time is continuous regardless of logging in or out. Account would expire when the ***Valid Period*** is used up or the quota depleted.

-**Quota** is the total period of time (xx days yy hrs zz mins), during which On-demand users are allowed to access the network. The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeeming.

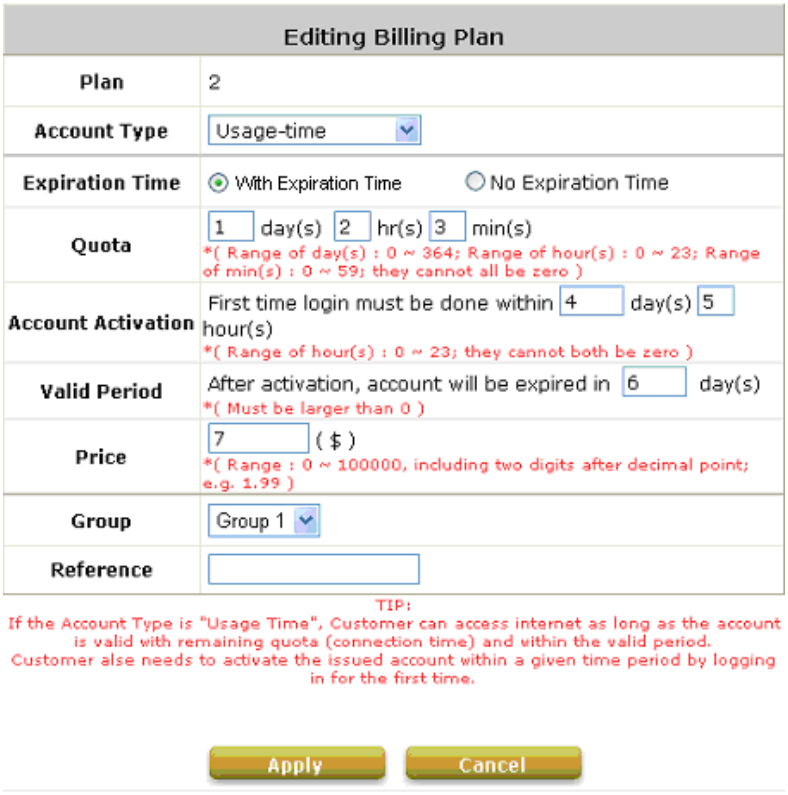
-**Account Activation** is carried out when the user logs in for the first time. Failing to do so in the period set in Account Activation will result in account expiration.

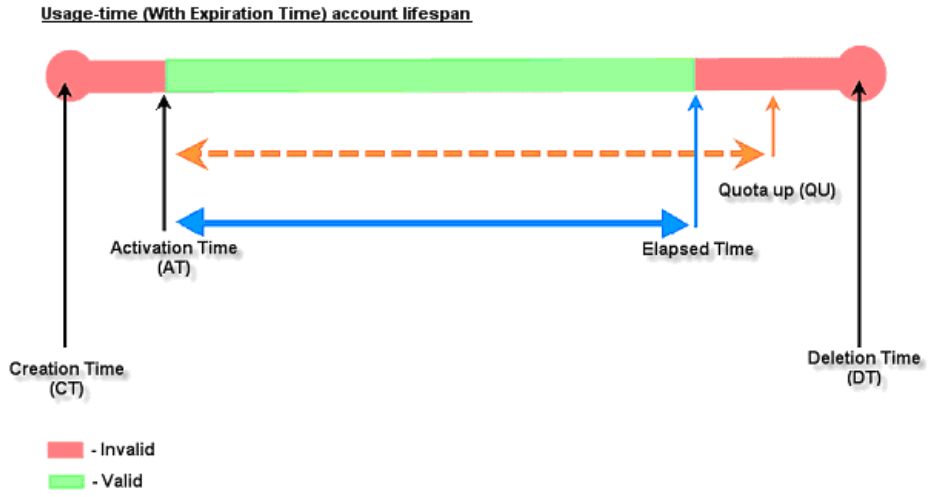
-**Valid Period** is the valid period of usage time. After this time period, even if there is remaining quota, the account will still expire.

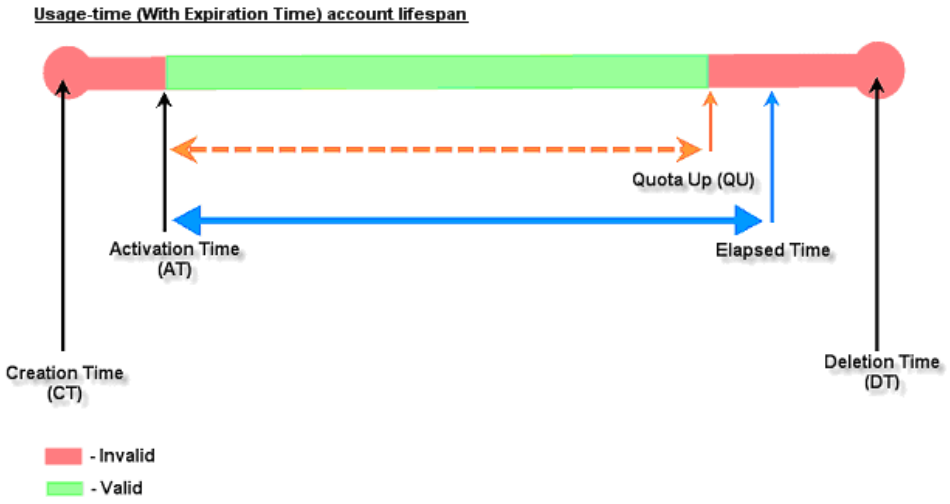
-**Price** is the unit price of this plan.

-**Group** will be the applied Group to users created from this plan.

-**Reference** field allows administrator to input additional information.


Editing Billing Plan
Plan
2
Account Type
Usage-time
Expiration Time
With Expiration Time
No Expiration Time
Quota
1 day(s) 2 hr(s) 3 min(s)
*(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)
Account Activation
First time login must be done within 4 day(s) 5 hour(s)
*(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period
After activation, account will be expired in 6 day(s)
*(Must be larger than 0)
Price
7 ($)
*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group
Group 1
Reference
TIP:
If the Account Type is "Usage Time", Customer can access internet as long as the account is valid with remaining quota (connection time) and within the valid period.
Customer alse needs to activate the issued account within a given time period by logging in for the first time.
Apply
Cancel





o**Usage-time with No Expiration Time:** Users can access internet as long as the account has remaining quota (usable time). Users need to activate the purchased account within the given time by logging in. It is ideal for short-term usage.

For example, in coffee shops, at airport terminals etc. This billing type only deducts quota while the user is using internet. Account will expire only when the quota is depleted.

-**Quota** is the total period of time (xx *days* yy *hrs* zz *mins*), during which On-demand users are allowed to access the network. The total maximum quota is "364Days 23hrs 59mins 59secs" even after redeeming.

-**Account Activation** is carried out when the user logs in for the first time. Failing to do so in the period set in Account Activation will result in account expiration.

-**Price** is the unit price of this plan.

-**Group** will be the applied Group to users created from this plan.

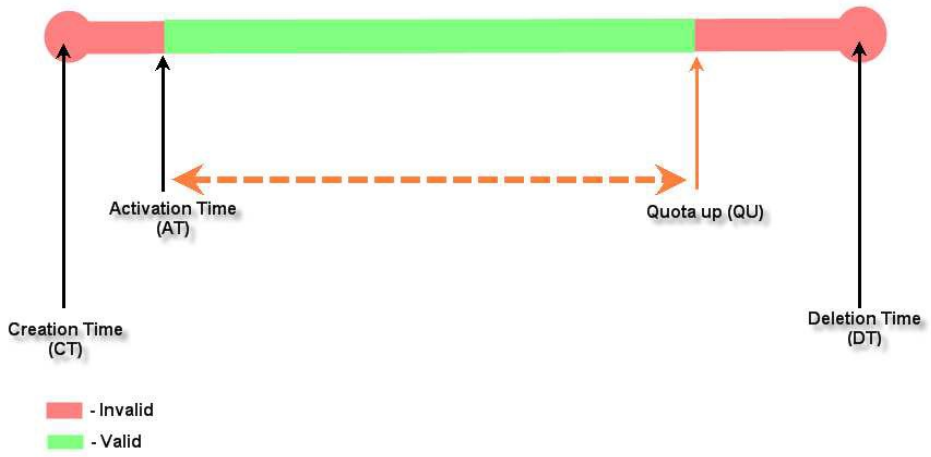
-**Reference** field allows administrator to input additional information.

Editing Billing Plan	
Plan	3
Account Type	Usage-time
Expiration Time	With Expiration Time / No Expiration Time
Quota	2 day(s) 3 hr(s) 4 min(s) *(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)
Account Activation	First time login must be done within 5 day(s) 6 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Price	7 ($) *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 1
Reference	

TIP:
If the Account Type is "Usage Time", Customer can access internet as long as the account is valid with remaining quota (connection time) and within the valid period.
Customer alse needs to activate the issued account within a given time period by logging in for the first time.

Apply Cancel

Usage-time (No Expiration) account lifespan



-**Hotel Cut-off-time: Hotel Cut-off-time** is the clock time (normally check-out time) at which the on-demand account is cut off (made expired) by the system on the following day or many days later.

On the account creation UI of this plan, operator can enter a Unit value which is the number of days to Cut-off-time according to customers' stay time.

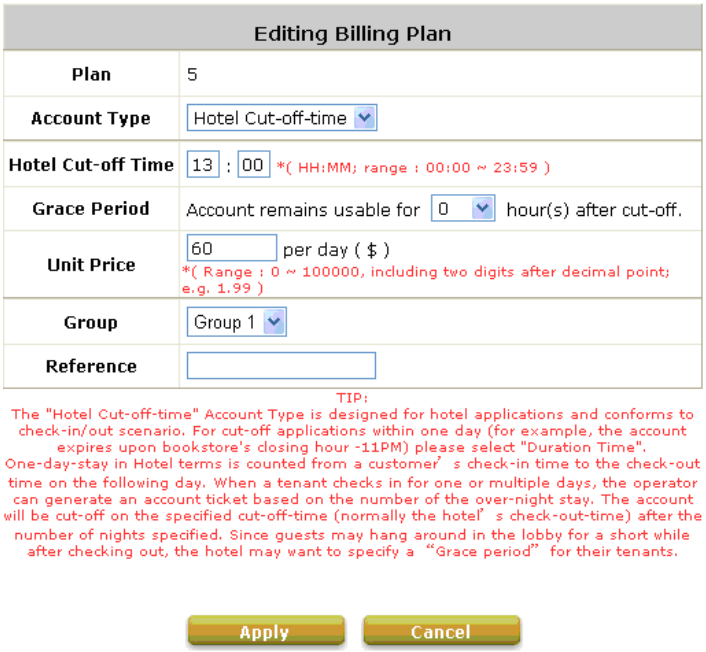
For example: Unit = 2 days, Cut-off Time = 13:00 then account will expire on 13:00 two days later.

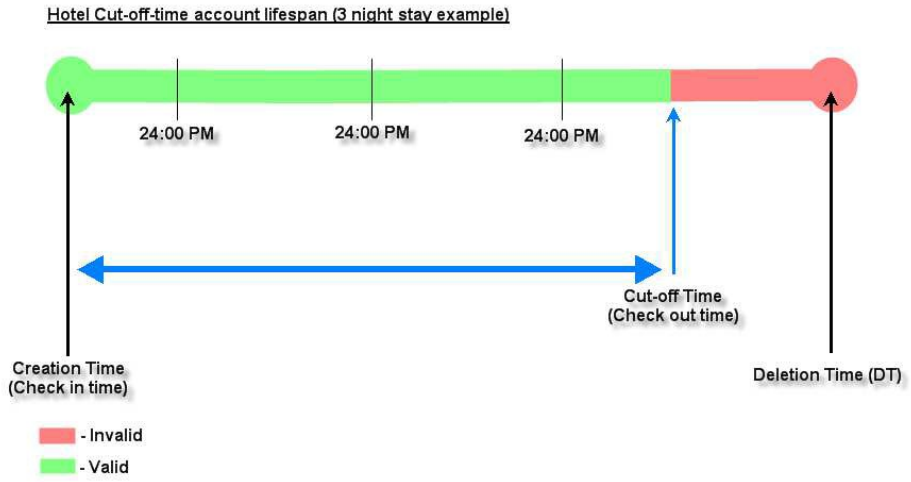
Grace Period is an additional, short period of time after the account is cut off that allows user to continue to use the on-demand account to access the Internet without paying additional fee.

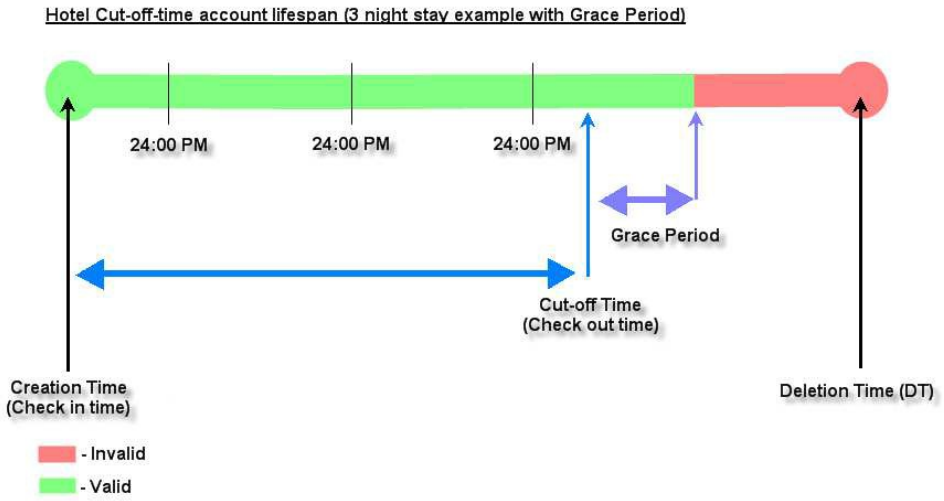
Unit Price is the daily price of this billing plan. It is mainly used in hostel (hotel?) venues to provide internet service according to guests' stay time.

Group will be the applied Group to users created from this plan.

Reference field allows administrator to input additional information.


Editing Billing Plan
Plan
5
Account Type
Hotel Cut-off-time
Hotel Cut-off Time
13 : 00 *(HH:MM; range : 00:00 ~ 23:59)
Grace Period
Account remains usable for 0 hour(s) after cut-off.
Unit Price
60 per day ($)
*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group
Group 1
Reference
TIP:
The "Hotel Cut-off-time" Account Type is designed for hotel applications and conforms to check-in/out scenario. For cut-off applications within one day (for example, the account expires upon bookstore's closing hour -11PM) please select "Duration Time".
One-day-stay in Hotel terms is counted from a customer's check-in time to the check-out time on the following day. When a tenant checks in for one or multiple days, the operator can generate an account ticket based on the number of the over-night stay. The account will be cut-off on the specified cut-off-time (normally the hotel's check-out-time) after the number of nights specified. Since guests may hang around in the lobby for a short while after checking out, the hotel may want to specify a "Grace period" for their tenants.
Apply
Cancel





Volume: Users can access internet as long as his/her account has remaining traffic volume quota.

The account will expire when *Valid Period* has been used up or the quota is depleted.

This type is ideal for small quantity of applications such as sending/receiving email, transferring a file, etc.

Count down of Valid Period is continuous regardless of logging in or out.

Quota is the total Mbytes (1~2000) On-demand users are allowed to use to access the network.

Account Activation is carried out when the user logs in for the first time. Failing to do so in the period set in Account Activation will result in account expiration

Valid Period is the valid period of usage time. After this time period, the account will expire even if there is remaining quota.

Price is the unit price of this plan.

Group will be the applied Group to users created from this plan.

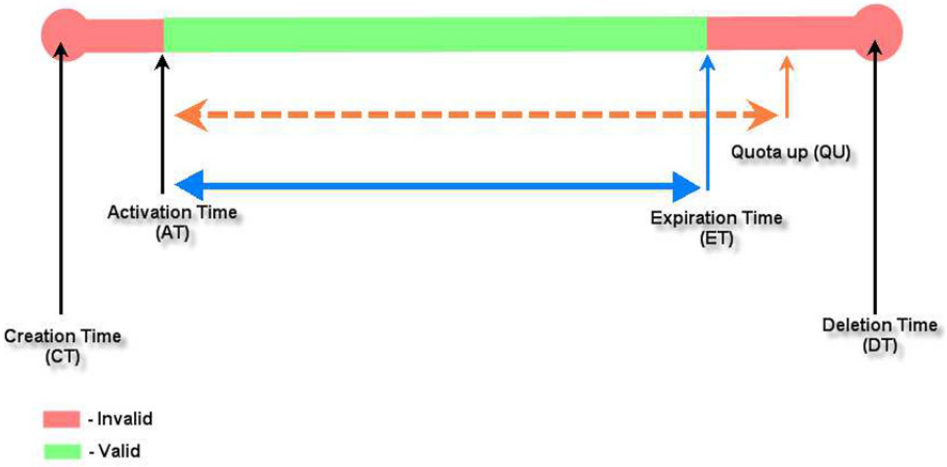
Reference field allows administrator to input additional information.

Editing Billing Plan	
Plan	1
Account Type	Volume
Quota	500 Mbyte(s) *(Range : 1 ~ 1000000)
Account Activation	First time login must be done within 1 day(s) 1 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 1 day(s) *(Must be larger than 0)
Price	1 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group	Group 4
Reference	

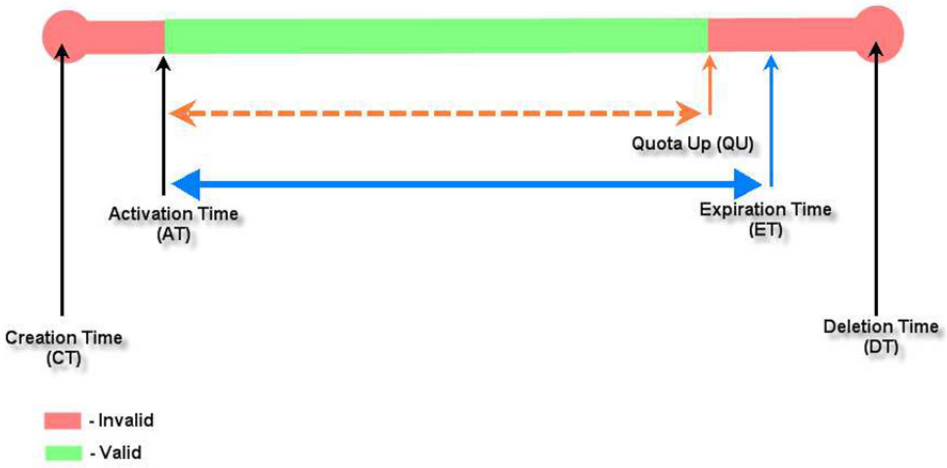
TIP:
If the Account Type is "Volume", Customer can access internet as long as the account is valid (within the valid period) with remaining quota (traffic volume).
Customer also needs to activate the issued account within a given time period by logging in for the first time.

Apply Cancel

Volume account lifespan



Volume account lifespan



Duration-time with Elapsed Time: Account is activated upon the account creation time. Countdown begins immediately after account creation and is continuous regardless of logging in or out. The account will expire once the *Elapsed Time* is reached. This billing type is ideal for providing internet service immediately after account creation throughout a specific period of time.

Begin Time is the time that the account will be activated for use. It is set to account creation time.

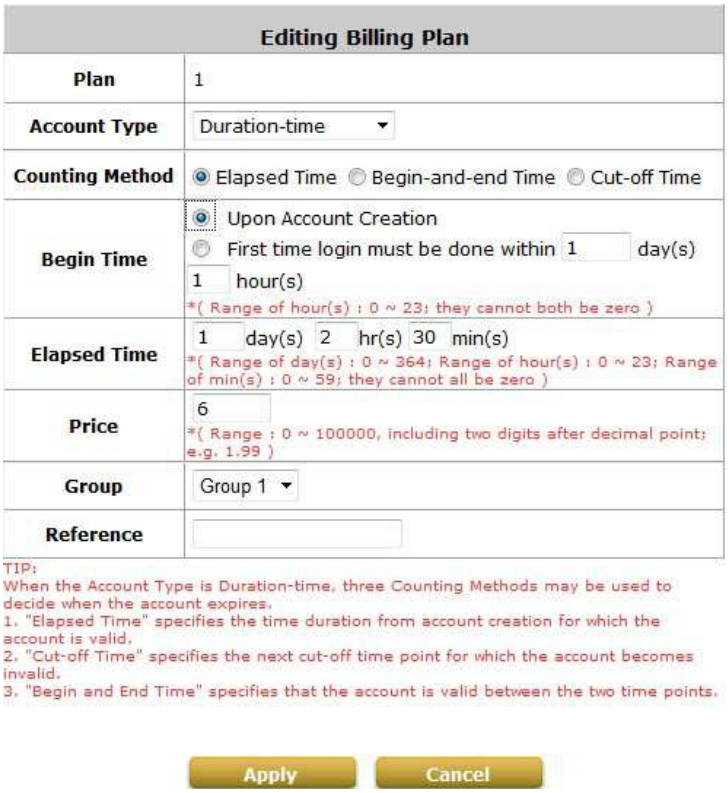
First time login is set to require users to log in within a specified period of time.

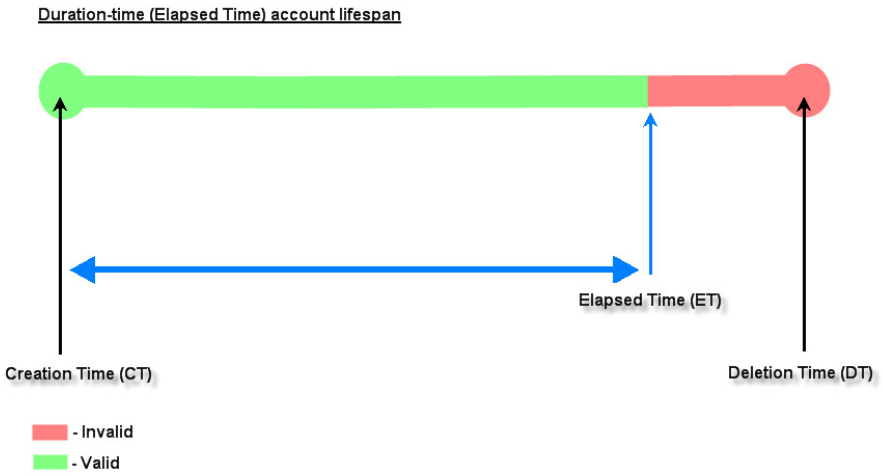
Elapsed Time is the time interval for which the account is valid for internet access (xx *hrs* yy *mins*).

Price is the unit price of this plan.

Group will be the applied Group to users created from this plan.

Reference field allows administrator to input additional information.


Editing Billing Plan
Plan
1
Account Type
Duration-time
Counting Method
Elapsed Time
Begin-and-end Time
Cut-off Time
Begin Time
Upon Account Creation
First time login must be done within 1 day(s)
1 hour(s)
*(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Elapsed Time
1 day(s) 2 hr(s) 30 min(s)
*(Range of day(s) : 0 ~ 364; Range of hour(s) : 0 ~ 23; Range of min(s) : 0 ~ 59; they cannot all be zero)
Price
6
*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group
Group 1
Reference
TIP:
When the Account Type is Duration-time, three Counting Methods may be used to decide when the account expires.
1. "Elapsed Time" specifies the time duration from account creation for which the account is valid.
2. "Cut-off Time" specifies the next cut-off time point for which the account becomes invalid.
3. "Begin and End Time" specifies that the account is valid between the two time points.
Apply
Cancel



Duration-time with Cut-off Time: Cut-off Time is the clock time at which the on-demand account is cut off (made expired) by the system on that day. For example if a shopping mall closes at 23:00, operators selling on-demand tickets can use this plan to create a ticket set to be Cut-off on 23:00. If an account of this kind is created after the Cut-off Time, the account will automatically expire.

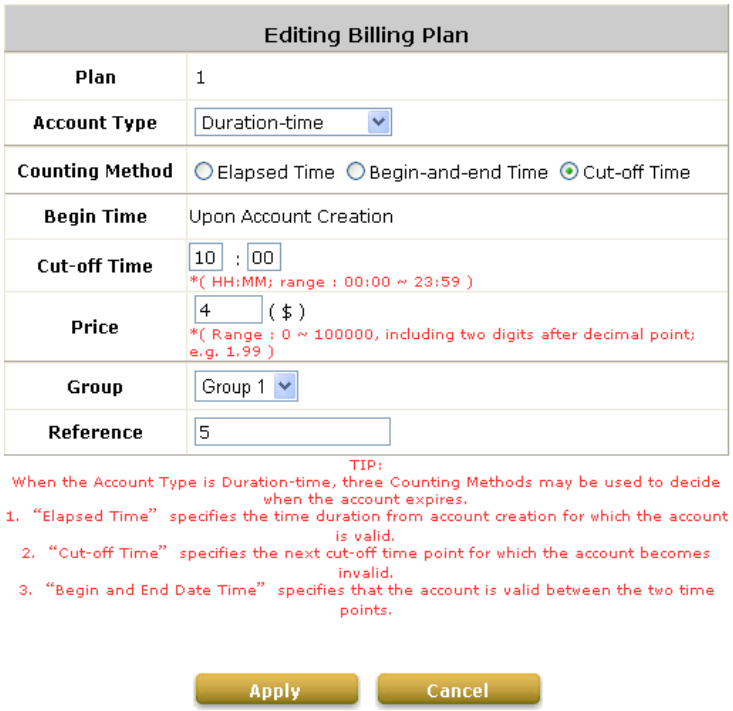
Begin Time is the time that the account will be activated for use. It is set to account creation time.

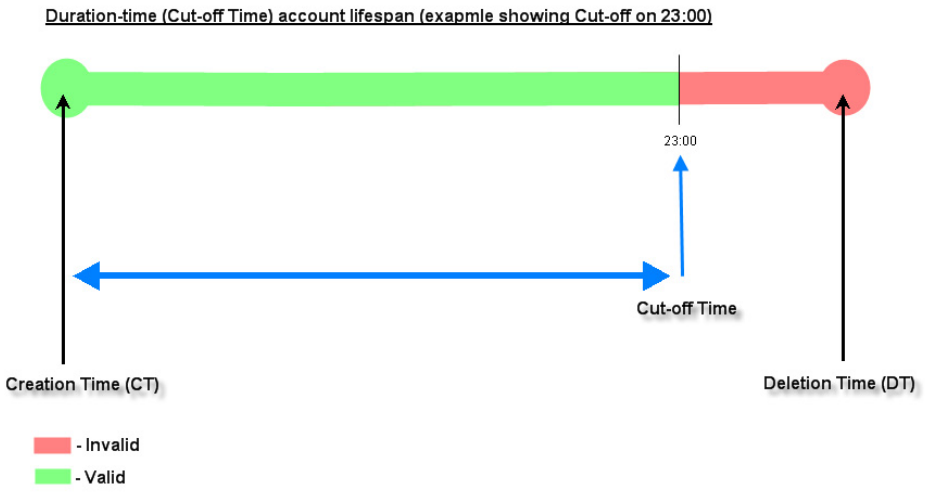
Cut-off Time is the clock time when the account will expire.

Price is the unit price of this plan.

Group will be the applied Group to users created from this plan.

·**Reference** field allows administrator to input additional information.


Editing Billing Plan
Plan
1
Account Type
Duration-time
Counting Method
Elapsed Time
Begin-and-end Time
Cut-off Time
Begin Time
Upon Account Creation
Cut-off Time
10 : 00
*(HH:MM; range : 00:00 ~ 23:59)
Price
4 ($)
*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group
Group 1
Reference
5
TIP:
When the Account Type is Duration-time, three Counting Methods may be used to decide when the account expires.
1. "Elapsed Time" specifies the time duration from account creation for which the account is valid.
2. "Cut-off Time" specifies the next cut-off time point for which the account becomes invalid.
3. "Begin and End Date Time" specifies that the account is valid between the two time points.
Apply
Cancel



Duration-time with Begin-and End Time: This plan defines explicitly the *Begin Time* and *End Time* of the account. Countdown begins immediately after account activation and expires when the *End Time* is reached. This plan is ideal for providing internet service throughout a specific period of time; for

example during exhibition events or large conventions where each registered participant will get an internet account valid from 8:00 AM Jun 1 to 5:00 PM Jun 5. Account can be created in batch similar to creating coupons.

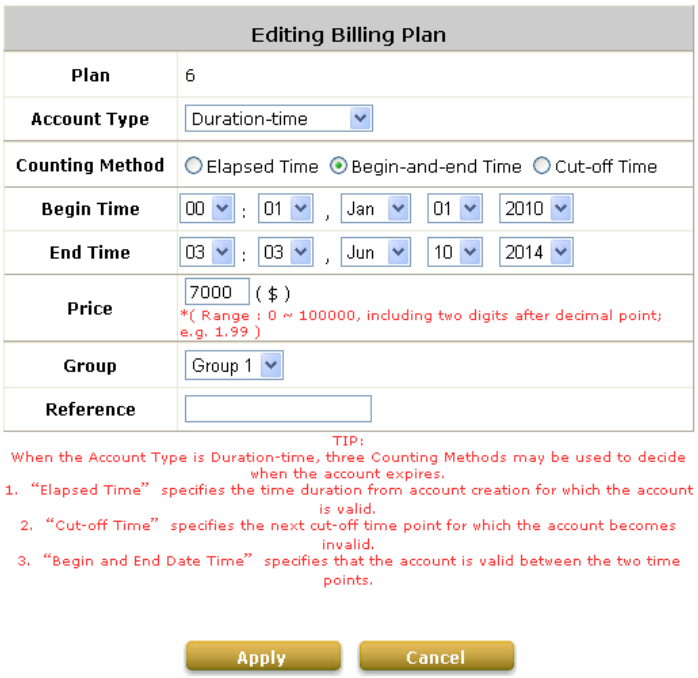
Begin Time is the time that the account will be activated for use, defined explicitly by the operator.

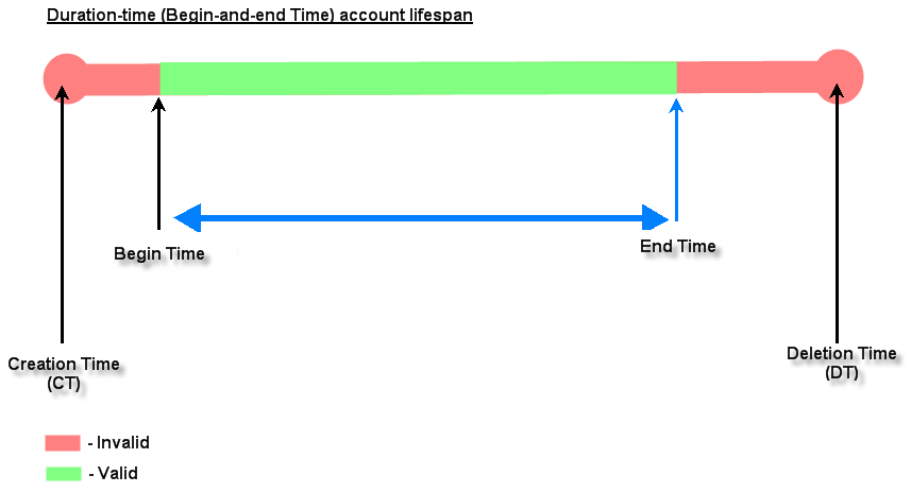
End Time is the time that the account will expire, defined explicitly by the operator.

Price is the unit price of this plan.

Group will be the applied Group to users created from this plan.

Reference field allows administrator to input additional information.


Editing Billing Plan
Plan
6
Account Type
Duration-time
Counting Method
Elapsed Time
Begin-and-end Time
Cut-off Time
Begin Time
00 : 01 , Jan 01 2010
End Time
03 : 03 , Jun 10 2014
Price
7000 ($)
*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Group
Group 1
Reference
TIP:
When the Account Type is Duration-time, three Counting Methods may be used to decide when the account expires.
1. "Elapsed Time" specifies the time duration from account creation for which the account is valid.
2. "Cut-off Time" specifies the next cut-off time point for which the account becomes invalid.
3. "Begin and End Date Time" specifies that the account is valid between the two time points.
Apply
Cancel



Appendix E. External Payment Gateways

This section is to show independent Hotspot owners how to configure related settings in order to accept payments via Authorize.net, PayPal, SecurePay or WorldPay, making the Hot Spot Wi-Fi an e-commerce environment for end users to pay for and obtain Internet access with credit cards.

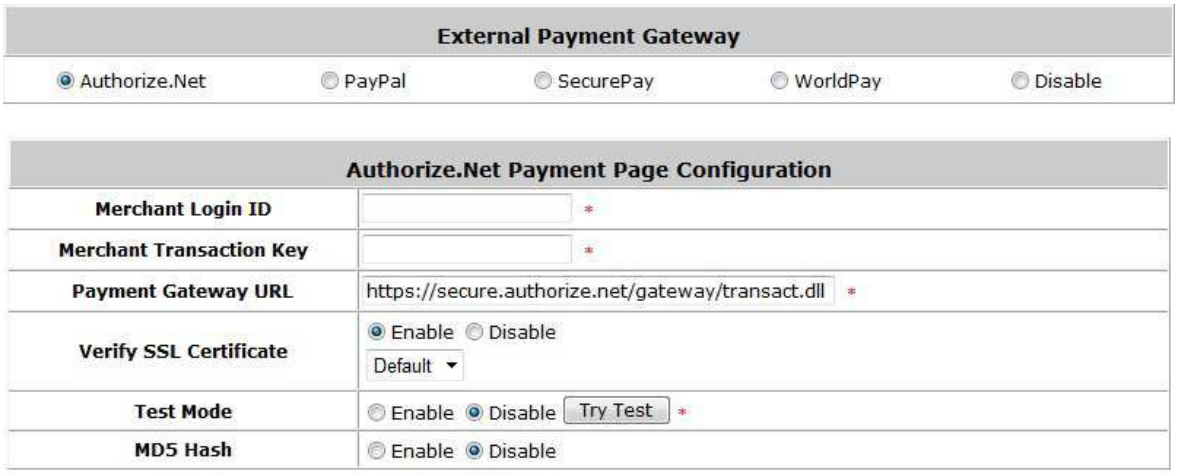
1. Payments via Authorize.Net

To configure Payments via Authorize.Net, go to:

Users >> Authentication >> On-demand User >> External Payment Gateway >> Authorize.Net.

Before setting up "Authorize.Net", it is required that the merchant owners have a valid Authorize.Net account.

> **Authorize.Net Payment Page Configuration**



Merchant ID: This is the "Login ID" that comes with the Authorize.Net account

Merchant Transaction Key: The merchant transaction key is similar to a password and is used by Authorize.Net to authenticate transactions.

Payment Gateway URL: This is the default website address to post all transaction data.

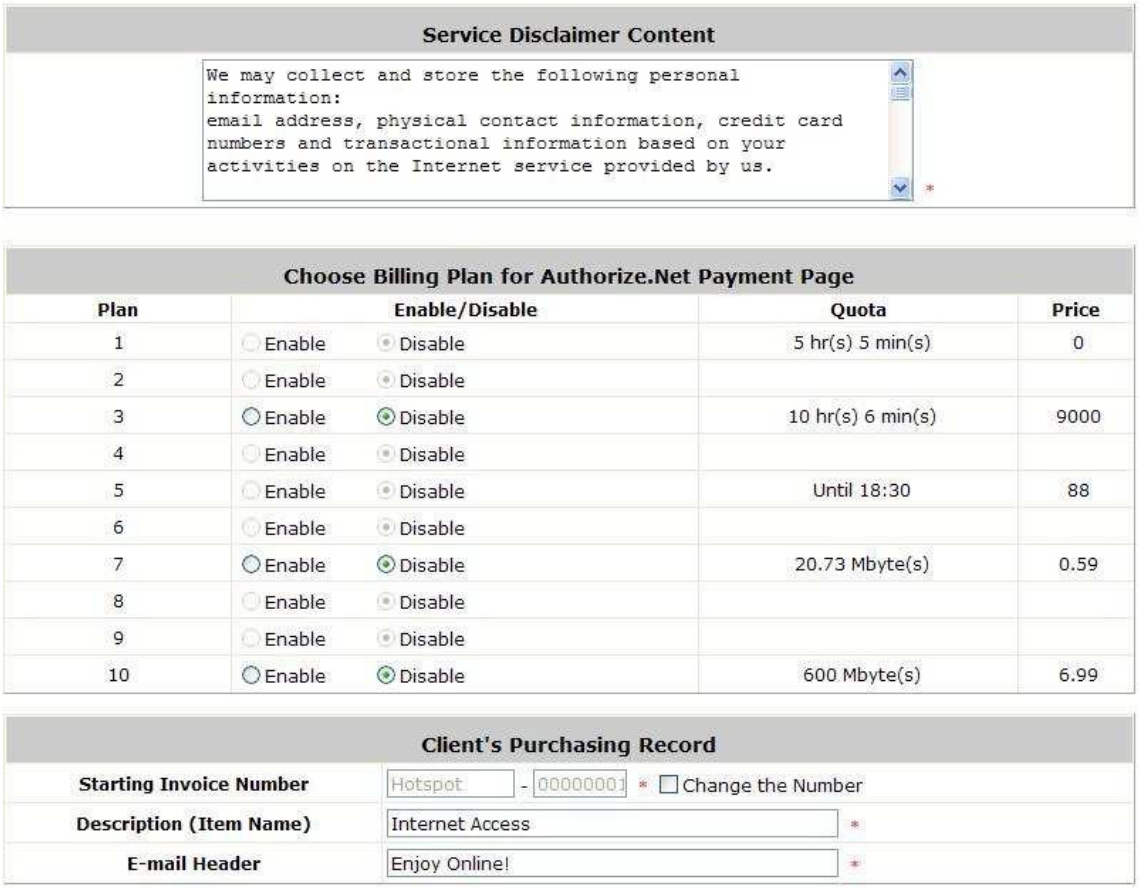
Verify SSL Certificate: This is to help protect the system from accessing a website other than Authorize.Net.

Test Mode: In this mode, merchants can post **test** transactions **for free** to check if the payment function works properly.

MD5 Hash: If transaction responses need to be encrypted by the Payment Gateway, enter and confirm a MD5 Hash Value and select a reactive mode.

The MD5 Hash security feature enables merchants to verify that the results of a transaction or transaction response received by their server are actually sent from the Authorize.Net.

> **Service Disclaimer Content/ Choose Billing Plan for Authorize.Net Payment Page/Client's Purchasing Record**



Service Disclaimer Content

We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us. *

Choose Billing Plan for Authorize.Net Payment Page

Plan	Enable/Disable	Quota	Price
1	Enable Disable	5 hr(s) 5 min(s)	0
2	Enable Disable		
3	Enable Disable	10 hr(s) 6 min(s)	9000
4	Enable Disable		
5	Enable Disable	Until 18:30	88
6	Enable Disable		
7	Enable Disable	20.73 Mbyte(s)	0.59
8	Enable Disable		
9	Enable Disable		
10	Enable Disable	600 Mbyte(s)	6.99

Client's Purchasing Record

Starting Invoice Number	Hotspot - 00000001 * Change the Number
Description (Item Name)	Internet Access *
E-mail Header	Enjoy Online! *

Service Disclaimer Content

View service agreements and fees for the standard payment gateway services here as well as adding a new or editing service disclaimer.

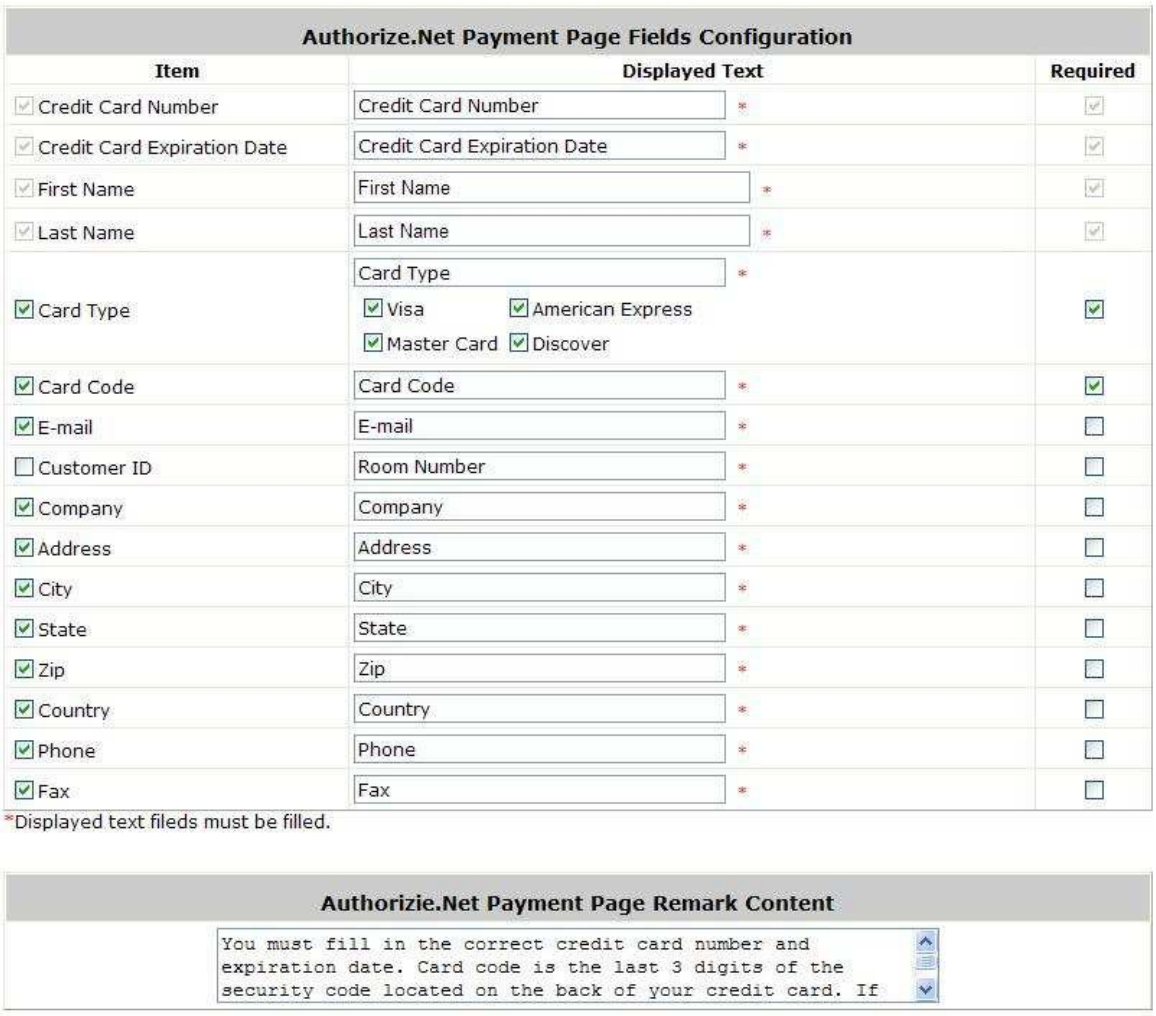
Choose Billing Plan for Authorize.Net Payment Page

These 10 plans are the plans configured in the **Billing Plans** page, and all previously enabled plans can be further enabled or disabled here, as needed.

Client's Purchasing Record

- **Starting Invoice Number:** An invoice number may be provided as additional information for a transaction. The number will be incremented automatically for each following transaction. Click the "Change the Number" checkbox to change it.
- **Description (Item Name):** This is the item information to describe the product (for example, Internet Access).
- **Email Header:** Enter the information that should appear in the header of the invoice.

> **Authorize.Net Payment Page Fields Configuration/ Authorize.Net Payment Page Remark Content**



Authorize.Net Payment Page Fields Configuration

Item	Displayed Text	Required
Credit Card Number	Credit Card Number *	
Credit Card Expiration Date	Credit Card Expiration Date *	
First Name	First Name *	
Last Name	Last Name *	
Card Type	Card Type * Visa American Express Master Card Discover	
Card Code	Card Code *	
E-mail	E-mail *	
Customer ID	Room Number *	
Company	Company *	
Address	Address *	
City	City *	
State	State *	
Zip	Zip *	
Country	Country *	
Phone	Phone *	
Fax	Fax *	

*Displayed text fileds must be filled.

Authorizie.Net Payment Page Remark Content

You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If

Authorize.Net Payment Page Fields Configuration

- **Item:** Check the box to show this item on the customer's payment interface.
- **Displayed Text:** Enter what needs to be shown for this field.
- **Required:** Check the box to indicate this item as a required field.
- **Credit Card Number:** Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.
- **Credit Card Expiration Date:** Expiration date of the credit card. This should be entered in the format of MMYY. For example, the expiration date of July September 2009 should be entered as 0709.
- **Card Type:** This value indicates the level of match between the Card Code entered in a transaction and the value that is on the file with a customer's credit card company. A code and narrative description are provided to indicate the results returned by the processor.
- **Card Code:** The three- or four-digit code assigned to a customer's credit card number (at the end of the credit card number found either on the front or back of the card).
- **E-mail:** An email address may be provided along with the billing information for a transaction. This is the customer's email address and should contain an @ symbol.

- **Customer ID:** This is an internal identifier for customers that may be associated with the billing information for a transaction. This information field may contain any format.
- **First Name:** The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.
- **Last Name:** The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.
- **Company:** The name of the company associated with the billing or shipping information entered on a given transaction.
- **Address:** The address entered either in the billing or shipping information of a given transaction.
- **City:** The city associated with either the billing address or shipping address of a transaction.
- **State:** A state associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.
- **Zip:** The ZIP code represents a five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.
- **Country:** The country associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full name.
- **Phone:** A phone number associated with both a billing and shipping address of a transaction.
- Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.
- **Fax:** A fax number may be associated with the billing information of a transaction. This number
- may be entered as all number or contain parentheses and dashes to separate the area code and number.

Authorizie.Net Payment Page Remark Content

Enter additional details for the transaction such as Tax, Freight and Duty Amounts, Tax Exempt status, and a Purchase Order Number, if applicable.

2. Payments via PayPal

To configure Payments via PayPal, go to:

User >> Authentication >> On-demand User >> External Payment Gateway >> PayPal.

Before setting up "PayPal", it is required that the hotspot owners have a valid PayPal "Business Account".

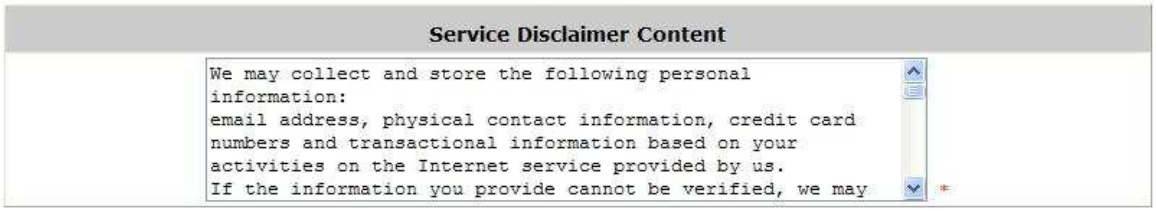
After opening a PayPal Business Account, the hotspot owners should find the **"Identity Token"** of this PayPal account to continue with "PayPal Payment Page Configuration".

> **External Payment Gateway / PayPal Payment Page Configuration**

PayPal Payment Page Configuration	
Business Account	*
Payment Gateway URL	https://www.paypal.com/cgi-bin/webscr *
Identity Token	*
Instant Payment Notification (IPN)	Enable Disable Behind NAT External Gateway IP: * External Gateway Port: *
Verify SSL Certificate	Enable Disable Default
Currency	USD (U.S. Dollar) *

- **Business Account:** The "Login ID" (an email address) associated with the PayPal Business Account.
- **Payment Gateway URL:** The default website address to post all transaction data.
- **Identity Token:** This is the key used by PayPal to validate all the transactions.
- **IPN behind NAT:** IPN is the acronym of Instant Payment Notification which is a mechanism adopted by PayPal for identifying the outcome of a transaction. When this option is enabled, an upstream NAT server may be designated for accepting the IPN message from PayPal. This is a mandatory configuration item if the WAN IP of your gateway in not a public IP address, corresponding NAT translation configurations are necessary.
- **Verify SSL Certificate:** This is to help protect the system from accessing a website other than PayPal
- **Currency:** The currency to be used for payment transaction.

> **Service Disclaimer Content / Choose Billing Plan for PayPal Payment Page**


Service Disclaimer Content
We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may

Choose Billing Plan for PayPal Payment Page

Plan	Enable/Disable	Quota	Price
1	Enable / Disable	5 hr(s) 5 min(s)	0
2	Enable / Disable		
3	Enable / Disable	10 hr(s) 6 min(s)	9000
4	Enable / Disable		
5	Enable / Disable	Until 18:30	88
6	Enable / Disable		
7	Enable / Disable	20.73 Mbyte(s)	0.59
8	Enable / Disable		
9	Enable / Disable		
10	Enable / Disable	600 Mbyte(s)	6.99

- **Service Disclaimer Content:** View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.
- **Choose Billing Plan for PayPal Payment Page:** These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

> **Client's Purchasing Record / PayPal Payment Page Remark Content**

PayPal Payment Page Remark Content
(A)Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button,

Client's Purchasing Record:

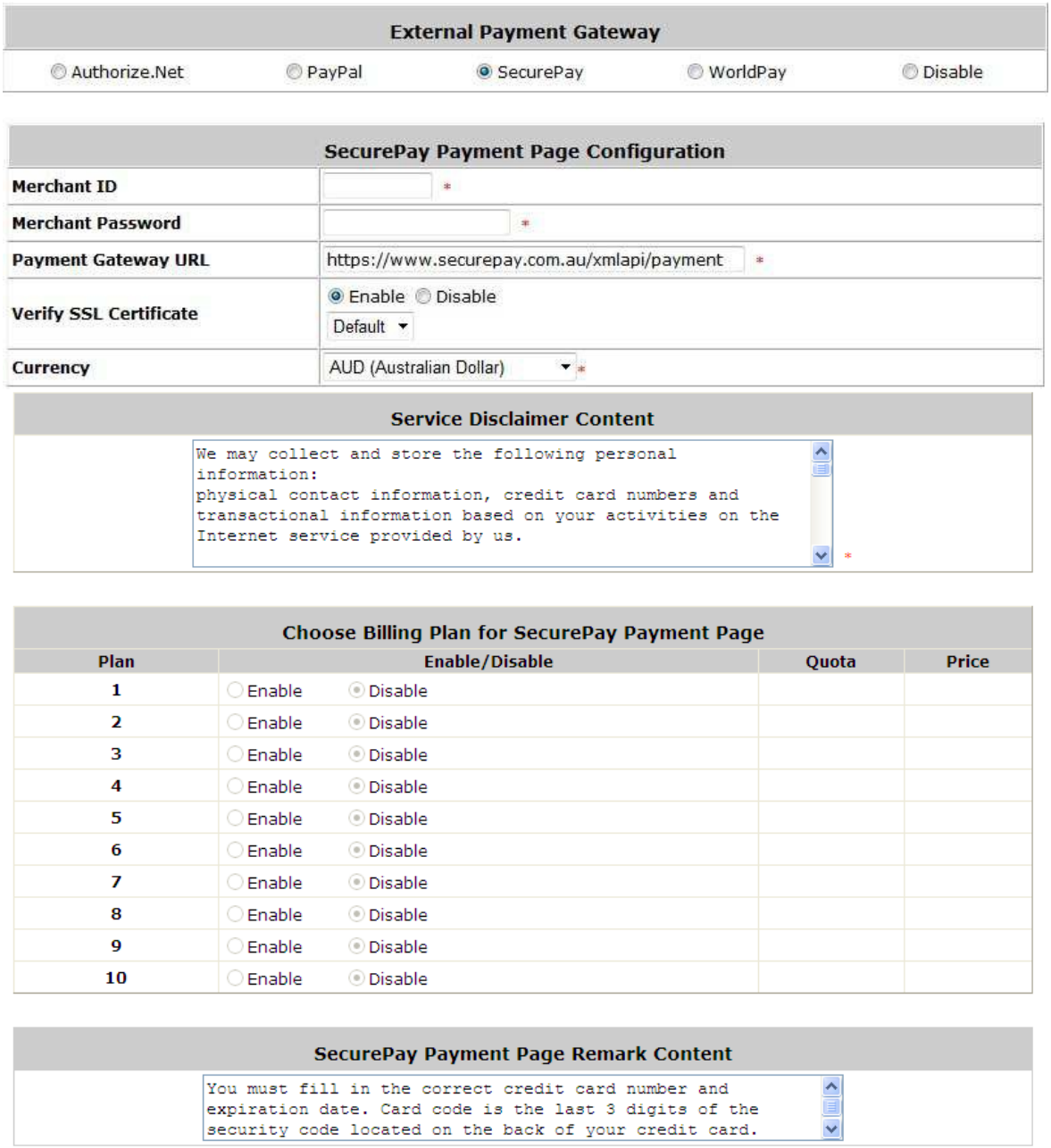
- **Starting Invoice Number:** An invoice number may be provided as additional information for the transaction. This is a reference field that may contain any sort of information.
- **Description:** Enter the product/service description (e.g. wireless access service).
- **Title for Message to Seller:** Enter the information that will appear in the header of the PayPal payment page.

PayPal Payment Page Remark Content: The message content will be displayed as a special notice to end customers in the page of "Rate Plan". For example, it can describe caution for making a payment via PayPal.

3. Payments via SecurePay

To configure Payments via SecurePay, go to: ***Users >> Authentication >> On-demand User>> External Payment Gateway >> SecurePay***.

Before setting up “SecurePay”, it is required that the hotspot owners have a valid SecurePay “Merchant Account” from its official website.



> **SecurePay Page Configuration**

Merchant ID: The ID that is associated with the Merchant Account.

Merchant Password: This is the key used by Secure Pay to validate all the transactions.

Payment Gateway URL: The default website address to post all transaction data.

Verify SSL Certificate: This is to help protect the system from accessing a website other than Secure Pay.

Currency: The currency to be used for the payment transactions.

> **Service Disclaimer Content**

View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

> **Choose Billing Plan for SecurePay Payment Page**

These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

> **SecurePay Payment Page Remark Content**

The message content will be displayed as a special notice to end customers.

4. Payments via World Pay

To configure Payments via WorldPay, go to:

Users >> Authentication >> On-demand User >> External Payment Gateway >> WorldPay.

WorldPayPaymentConfiguration	
WorldPayInstallationID	*
Payment Gateway URL	https://select.wp3.rbsworldpay.com/wcc/purchase *
Currency	GBP (Pound Sterling) *

Service Disclaimer Content
We may collect and store the following personal information: physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us. *

WorldPayBillingConfiguration			
Plan	**Enable/Disable**	**Quota**	**Price**
1	Enable Disable	15 min(s) connection time quota with expiration	10.91
2	Enable Disable	11 min(s) connection time quota	1
3	Enable Disable	Valid until 12:00 the following day	5
4	Enable Disable	Valid from 2010/07/14 12:00:00 till 2010/07/14 23:59:00	1
5	Enable Disable		
6	Enable Disable		
7	Enable Disable		
8	Enable Disable		
9	Enable Disable		
10	Enable Disable		

WorldPayNoteContent
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card.

> **WorldPay Payment Configuration**

WorldPayInstallation ID: The ID of the associated Merchant Account. **Payment Gateway URL:** The default website of posting all

transaction data. **Currency:** The currency to be used for the payment transactions.

> **Service Disclaimer Content**

View the service agreement and fees for the standard payment gateway services as well as add or edit the service disclaimer content here.

> **WorldPay Billing Configuration**

These 10 plans are the plans in **Billing Configuration**, and the desired plan(s) can be enabled.

> **WorldPay Note Content**

The message content will be displayed as a special notice to end customers.

Before setting up “WorldPay”, it is required that the hotspot owners have a valid WorldPay “Merchant Account” from its official website: RBS WorldPay: Merchant Services & Payment Processing, going to ***rbsworldpay.com >> support center >> account login***.

STEP1. Log in to the Merchant Interface.

> Login url: www.rbsworldpay.com/support/index.php?page=login&c=WW
> Select Business Gateway - Formerly WorldPay
> Click Merchant Interface
> Username: user2009
> Password: user2009

STEP2. Select Installations from the left hand navigation
STEP3. Choose an installation and select the Integration Setup button for the specific environment.

> Installation ID: 239xxx

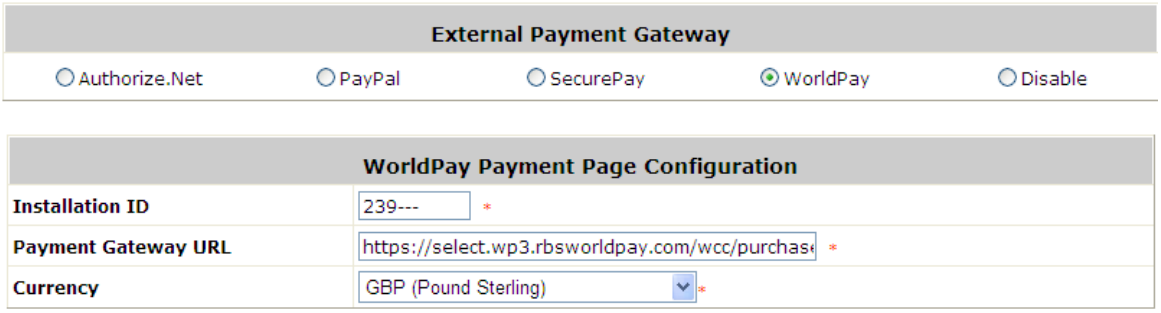
STEP4. Check Enable Payment Response checkbox.
STEP5. Enter the Payment Response URL.

> URL : <wpdisplay item=MC_callback>

STEP6. Check Enable the Shopper Response.

STEP7. Select the Save Changes button
STEP8. Input Installation ID and Payment Gateway URL in gateway UI.

> Installation ID: 2009test
> URL : https://select.wp3.rbsworldpay.com/wcc/purchase



Note: *The WAN IP of gateway must be a real IP.*

Appendix F. Portal Page Customization

Since every Service Zone have their own configuration profiles and acts like a virtual gateway, administrators can customize or define their own portal pages utilized by users of that Service Zone.

The customizable pages of a Service Zone are: **Disclaimer Page, Login Page, Logout Page, Login Success Page, Login Fail Page, Logout Success Page, Logout Fail Page, Login Success Page for On-demand User, Port Location Mapping Free Login Page, Port Location Mapping Charge Login Page.**

Custom Pages	Disclaimer Page	Configure
	Login Page	Configure
	Logout Page	Configure
	Login Success Page	Configure
	Login Failed Page	Configure
	Login Success Page for On-demand User	Configure
	Logout Success Page	Configure
	Logout Failed Page	Configure

Main Menu >> System>Service Zone >> Service Zone Configuration

For each customizable page, the available customization options are to use: **Default Page, Template Page, Uploaded Page,** or **External Page.**

Login Page Selection for Users - Service Zone: Default	
○ Default Page	○ Template Page
○ Uploaded Page	◉ External Page

Main Menu >> System >> Service Zone >> Service Zone Configuration >> Login Page

Default Page uses a web page stored within the system, its format and content cannot be changed.

Template Page also uses a web page stored within the system, but the contents such as text color, background color displayed text and logo can be configured according to your preferences.

Uploaded Page is to upload yourself defined web page into the system, and use it as portal page displayed to the user.

External Page uses a web page stored in an external web server as the portal page for your users.

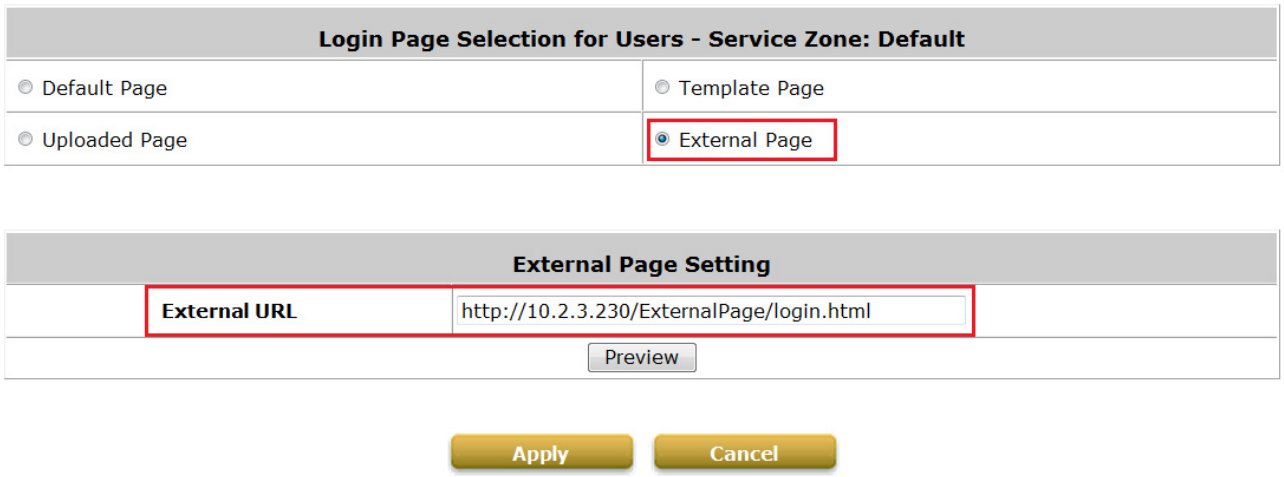
Because the pages are located on a remote server, therefore special efforts are required by these external pages to parse, process and send necessary URL parameters to and from the system.

Since External Pages needs more attention and care to setup, its html codes also need to include mechanisms for processing the necessary URL parameters, please refer to further details regarding on external pages in the following sections.

How External Pages Operate

Choose ***External Page*** if you desire to use an external web page for your custom pages.

Simply enter the URL of your external webpage, click ***Preview*** button to check if it is reachable, take a look at how your external webpage will be displayed, then click ***Apply*** button.



Main Menu >> System >> Service Zone >> Service Zone Configuration >> Login Page

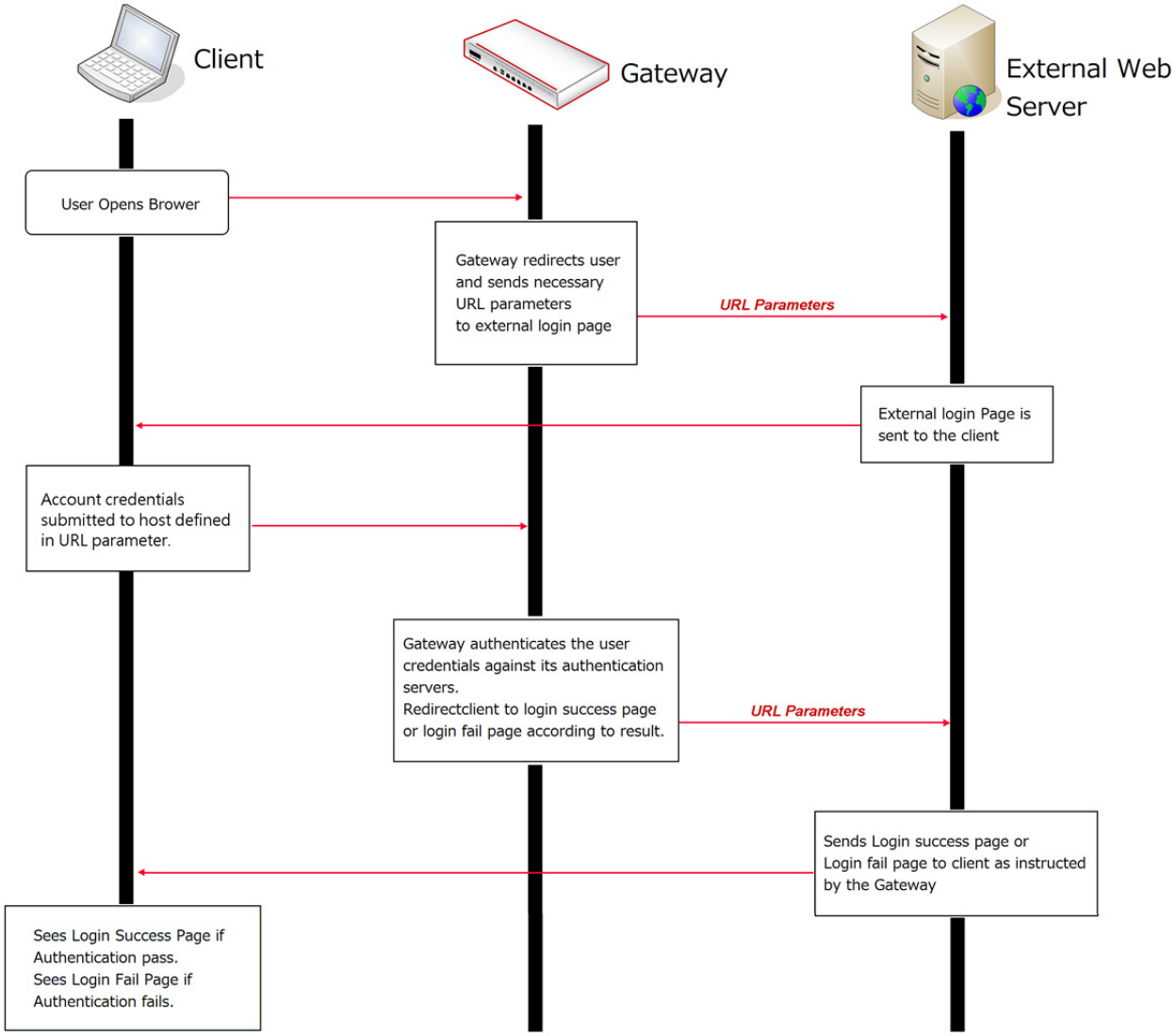
When a user connects to this Service Zone, opens a web browser and attempts to access the internet, the system will redirect the user to the external login page configured.

Gateway while redirecting users to the external web page will also send URL parameters required for the operation, for instance user authentication. Therefore, each self-defined external pages (*Login, Logout, Login Success, Logout Success,* etc.) requires codes to handle **URL parameters** to and from the Gateway.

A simple example is illustrated below for Login Page, please refer to **External Login Page Parameters** for URL parameter relating to other pages such as *Login Success Page* ... and etc.

Therefore it is important that your external pages are designed by someone with good knowledge of URL parameter utilization.

Diagram below explains how External Page operates using user login flow as illustration:


Client
Gateway
External Web Server
User Opens Brower
Gateway redirects user and sends necessary URL parameters to external login page
URL Parameters
External login Page is sent to the client
Account credentials submitted to host defined in URL parameter.
Gateway authenticates the user credentials against its authentication servers.
Redirectclient to login success page or login fail page according to result.
URL Parameters
Sends Login success page or Login fail page to client as instructed by the Gateway
Sees Login Success Page if Authentication pass.
Sees Login Fail Page if Authentication fails.

The URL parameters sent by the Gateway to the external login page are as follows:

Field	Value	Description
loginurl	String (URL encoded)	The URL which shall be submitted when user login.
remainingurl	String (URL encoded)	The URL which shall be submitted when user want to get remaining quota.
vlanid	Integer (1 ~ 4096)	VLAN ID
gwip	IP format	Gateway activated WAN IP address
client_ip	IP format	Client IP address
umac	MAC format (separated by ':')	Client MAC address
session	String	Encrypted session information, include: client IP address, MAC address, date, and return URL.

You will need to parse the required parameters in your html code. The following HTML code segment is an example of parsing *loginurl* parameter with a self define javascrip function:

```
<FORM action="" method="post" name="form">
```

```
<script language="Javascript">
form.action = getVarFromURL(window.location.href, 'loginurl');
</script>
<INPUT type="text" name="myusername" size="25">
<INPUT type="password" name="mypassword" size="25">
<INPUT name="button_submit" type="submit" value="Enter">
<INPUT name="button_clear" type="button" value="Clear">
</FORM>
```

The following shows the corresponding self-defined javascript function used to parse the *loginurl* parameter:

```
function getVarFromURL(url, name) {
if(name == "" || url == "") { return ""; }
name = name.replace(/[\[]/|"\\\[").replace(/[\]]/|"\\\]");
var regObj = new RegExp("[\\?&]"+name+"=([^&#]*)");
var result = regObj.exec(url);
if(result == null) { return ""; }
else { return decodeURIComponent(result[1]); }
}
```

Appendix G. Terminal Server Setup

Overview of Network Ticket Generator

RT-TO696RF is an innovative product RayTalk offers to facilitate the communication between Hot Spot Wi-Fi Access Point and Internet Subscriber Gateway and serial POS printer.

It is mainly used to have the connected printer fast-print necessary account information extracted from Hot Spot Wi-Fi Access Point or Internet Subscriber Gateway for a user who would like to access the Internet or managed networks, making provisioning of wired or wireless connection easier and more user-friendly.

What is noteworthy is that, RT-TO696RF supports wireless connectivity to the uplink gateway.

That is, operators now can deploy a network with lesser physical wires.

Here is a deployment example:

Useful Shortcut Keys

Combination	Function
'Number' + ENTER	To create and print out an on-demand account of an enabled billing plan of the uplink Hot Spot Wi-Fi Access Point or Subscriber Gateway mainly for the user who purchased an account.
'Number 1' + 'asterisk (*)' + 'Number 2' + ENTER	Print a ticket of billing '**Number 1**' with '**Number 2**' units. For example, **'8' + asterisk(*) + '3' + ENTER** is equal to create an on-demand account of billing plan 8 with 3 units and have the POS printer print out the corresponding ticket. That is, the quota that billing plan 8 grants is multiplied by 3.
FUNC + '1' + ENTER	To print out the information of RT-TO696RF, including (1) its IP address (2) the firmware version and the build number (3) the current listening port (4) uplink connection status (5) the IP address of the uplink Hot Spot Wi-Fi Access Point or Subscriber Gateway.
FUNC + ENTER	To clear what is pressed. This is used when the operator pressed a wrong button or combination. The system will also clear it automatically after five seconds.
FUNC + '0' + ENTER	To activate Safe Mode – disabling the **FUNC + '1' + ENTER** shortcut key in order to protect RT-TO696RF's information leakage.
'4-digit' + ENTER	To unlock Safe Mode. This 4-digit password can be changed on the WMI at "System >> Safe Mode (Password)." The default value is '**0000**.'
'asterisk (*)' + ENTER	To lock the keypad, excluding the TAS and the Reset button. In Lock Mode, the **Status** indicator will enter into special flashing. Press asterisk (*) **+ ENTER** again to disable the function, and the LED indicator **Status** will go back to short illuminated intervals or long illuminated intervals.

LED Panel

LED indicators

Power

When the power adapter is connected, **Power** will become constantly on; when disconnected, the light turns into constantly off.

Always check if **Power** is on before using RT-TO696RF.

Status

1. Short illuminated intervals means RT-TO696RF successfully booted up. It flashes slowly.

2. Long illuminated intervals means RT-TO696RF and uplink device connected

3. Special flashing means the keypad locked. The indicator fast-blinks twice periodically.

Note: <TAS Mode only>

4. Fast flashing means RT-TO696RF *trying to connect to uplink device.*

5. Constantly off for ten seconds means RT-TO696RF *fails to connect to uplink device after step 4. Afterwards,* ***Status*** *will go back to step 1.*

6. Constantly on for ten seconds means RT-TO696RF *succeeds in connecting to uplink device after step 4. Afterwards,* ***Status*** *will go to step 2.*

Ethernet

Ethernet turns into constantly on when an Ethernet cable is connected.

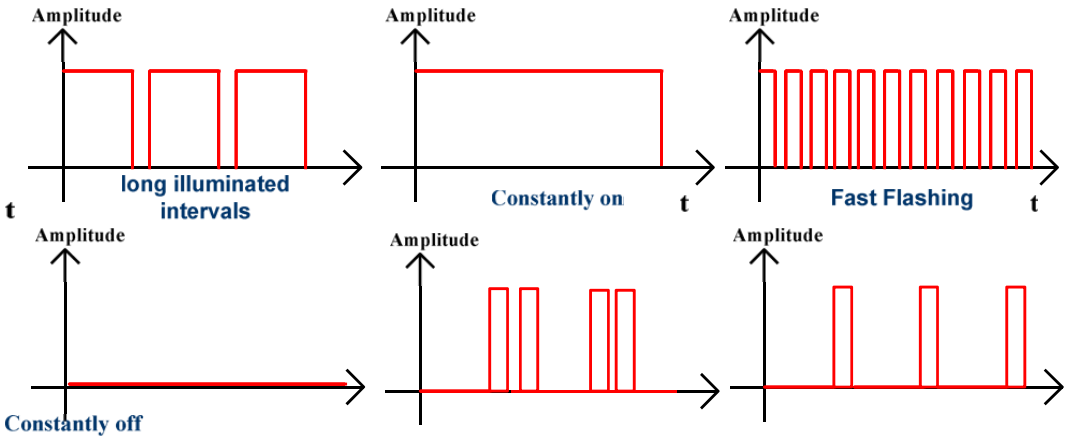
Ethernet blinks when the system detects wired traffic passing Ethernet. It is constantly off when no cable is connected.

WLAN

WLAN behaves similarly as Ethernet - becoming constantly on when wireless connectivity is enabled (not necessarily connected. It just means that the RF card is ready to serve). WLAN blinks when the system detects wireless traffic. It is constantly off if the RF card is disabled.

Understanding the LED indicators

There are four LED indicators on the panel : **Power**, **Status**, **LAN**, and **WLAN** from left to right. Below summarizes all indication types in different states:

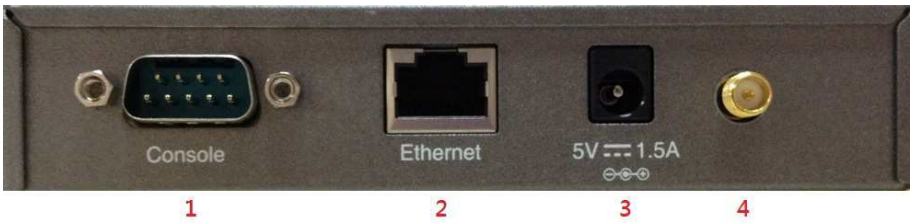


Right Side Panel Overview

Right Side Panel

1. Kensington Lock	Be used to lock the device to a pole.
2. Restart / Reset	Pole once to reboot the system. Poke for five seconds to make RT-TO696RF set back to factory default settings.
3. TAS	Terminal Auto Setup (TAS). Press three seconds to initiate the auto uplink connection process. This will be introduced later.

Left Side Panel Overview



Left Side Panel

1. Console	Serial port for connecting to a POS printer.
2. Ethernet	RJ-45 Ethernet port Serial port for connecting to the uplink gateway via wire.
3. 5V / 1.5A	The DC power socket for connecting to an external power source through a DC power supply.
4. Antenna connector	Assemble the dipole antenna within the package here.

Including RT-TO696RF into Your Network

1. Put relevant devices in place.
2. Attach a RT-TO696RF to a power adaptor provided in the package.
3. Attach a POS printer to a power adaptor provided in the package and turn on the power switch situated on the left side of the device.
4. Connect a POS printer to the Console port of RT-TO696RF by a RS-232 cable provided within the POS printer package.
5. Connect RT-TO696RF to your RayTalk Internet Subscriber Gateways via Ethernet port or wirelessly. If you are to do it wirelessly, conduct a site survey in the first place.
The wireless coverage is subject to change.
6. To verify if the deployment works fine. Press **FUNC + '1' + ENTER** to see if RT-TO696RF is attached to a correct gateway and get an IP address from it. Additionally, press 'Number' + **ENTER** to see if an account with a certain billing plan can be printed out. If it is not working properly, go to Appendix A for trouble shooting.

Managing RT-TO696RF on the Web Management Interface

RT-TO696RF is designed specifically to operate in conjunction with all RayTalk Hot Spot Wi-Fi Access Point and Internet Subscriber Gateways.

If you are not using default settings, before connecting RT-TO696RF to your RayTalk Hot Spot Wi-Fi Access Point and Internet Subscriber Gateways, some configurations steps are required.

Go to the Web Management Interface (WMI) for RT-TO696RF's relevant configurations.

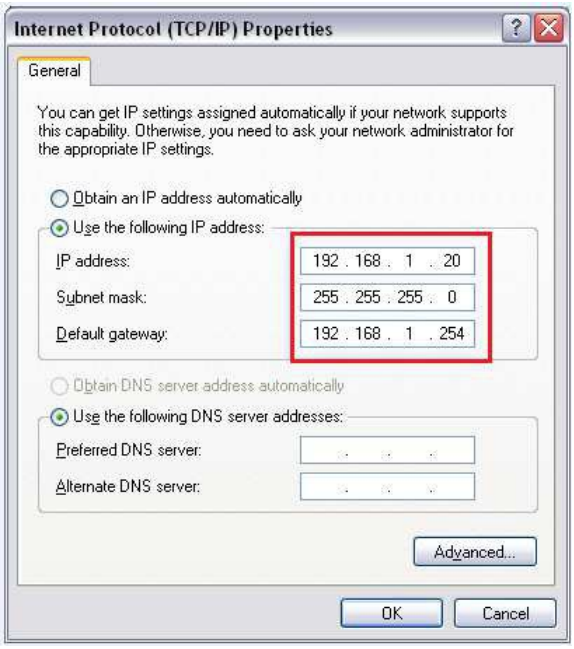
The default values are:

IP address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

Remember to set the TCP/IP settings of the computer you use with a static IP address that is under the same subnet as RT-TO696RF. For example: 192.168.1.20.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 20
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 1 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

The settings of RT-TO696RF are separated into seven categories, which are

1. **System** – to setup the system name and device control.
2. **Uplink** – to determine wired / wireless relevant parameters. Any change on this page will take effect after rebooting the system.
3. **Console** – to change console related settings for POS printers.
4. **Utility** – to upgrade the firmware version or backup/ restore RT-TO696RF's configuration settings.
5. **Password** – to change administrator's password.
6. **Reboot** – to reboot (restart) the system.
7. **Status** – to overview device, system, uplink, and radio status if available.

Setting Up RT-TO696RF with the POS Printer

Serial Settings

To make a POS printer properly functions with RT-TO696RF, set up serial settings in advance in **Console** on RT-TO696RF's WMI.

The default values are for RT-TP5x5 devices.

Change the values if you use another POS printer.

Printing On-demand Tickets for Your Customers

Operators have two ways of printing on-demand account tickets for their customers. One is to go onto the WMI of RayTalk Hot Spot Wi-Fi Access Point or Internet Subscriber Gateway. The other is to use RT-TO696RF by the following two shortcut keys.

(1) **'Number' + ENTER** or

(2) **'Number 1' + asterisk (*) + 'Number 2' + ENTER**

For example,

'**3**' + **ENTER** is to have POS printer print out a billing 3 ticket;

'4' + asterisk (*) + '2' + ENTER allows operator to print a single ticket of billing plan 4 with two units of the quota.

That is, the given quota is multiplied by two. Note that the keys can only print out tickets one at a time.

To Batch-create tickets, turn to

Main Menu > Users > Authentication > On-demand User Server Configuration > On-demand Account Batch Creation on RayTalk Hot Spot devices's WMI.

Use **FUNC + ENTER** or wait 5 seconds to clear the wrong number just pressed.

Setting up RT-TO696RF with the RayTalk Hot Spot Wi-Fi Access Point or Internet Subscriber Gateway

RT-TO696RF offers 'manual' and 'auto' connection to uplink RayTalk Hot Spot Wi-Fi Access Point or Internet Subscriber Gateway. The former implies that administrator would have to go on to RT-TO696RF's WMI, filling in necessary columns that are supposed to fit what is set up on the controller end. However, the auto connection – called Terminal Auto Setup (TAS) – is particularly designed for quickly establishing connection without any previous setting.

Manual setup

Connecting RT-TO696RF to uplink RayTalk Hot Spot Wi-Fi Access Point or Internet Subscriber Gateway manually, there are still two ways to achieve. One is through wired connection, and the other is via wireless connection.

Method 1: Wired Connection

Plug in an Ethernet cable between RT-TO696RF and RayTalk Hot Spot Wi-Fi Access Point or Internet Subscriber Gateway. Fill in Network Settings and make sure they match what is determined on the controller. The change will take effect after (1) clicking **Save** and (2) rebooting the system. After RT-TO696RF and the uplink device has built up a successful connection, the **Status** indicator will blink with long illuminated intervals.

Method 2: Wireless Connection

Fill in Network Settings and Wireless Settings, click **Save,** and reboot the system. After RT-TO696RF and the uplink device has successfully built up a connection, the **Status** indicator will blink with long illuminated intervals.

Note: When wired connection is established, the wireless connectivity will be turned off by the system automatically, meaning wireless and wired connection will not co-exist at any time.

Wired connection has a higher priority.

When the settings are done completely on the RayTalk Hot Spot Wi-Fi Access Point or Internet Subscriber Gateway side, go to RT-TO696RF's WMI and check if every uplink setting matches that on the controller.

Terminal Auto Setup (TAS – Only available on RT-TO696RF)

TAS refers to an automatic connection mechanism that requires **NO previous network settings**. Just press the

TAS button on RT-TO696RF for three seconds, and it will automatically look for and associate to a suitable RayTalk Hot Spot Wi-Fi Access Point or Internet Subscriber Gateway that supports this function.

The TAS connection will rewrite the previous manual settings. You will see the **Uplink** page of the WMI grayed out as well as **Status** show that the system is in TAS mode.

TAS process takes about thirty seconds for completion. Whether the connection succeeds or fail s the attempt, RT-TO696RF will always have the printer print out if the connection is 'successful' or it 'failed.' Please make sure beforehand that the Ethernet cable is plugged the wireless environment is ok.

For more information visit
www.raytalk.com - info@raytalk.com
RayTalk Industries S.r.l via N. di Galasso, 19 - Zona Ind.le Galazzano - 47899 Serravalle - Rep. di San Marino (RSM)
Tel: 0549-901170 / Fax: 0549-900890 / Country code: +378

Copyright © RayTalk Industries. All rights reserved. Every object or process described in this document is owned by Industries RayTalk except as expressly discussed and referred to third parties. No part of this document or description herein may be reproduced, used, engineered, transferred or made available to any person by any form or by any means without the express written permission of the authors and RayTalk Industries. All specifications are subject to change without notice. Any violation will be prosecuted under existing laws. All specifications may change without notice.